(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001年10月11日 (11.10.2001)

PCT

(10) 国際公開番号
WO 01/76127 A1

(51) 国際特許分類[7]: H04L 9/00, G11B 20/10, 20/12

(21) 国際出願番号: PCT/JP01/02928

(22) 国際出願日: 2001年4月4日 (04.04.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2000-101862 2000年4月4日 (04.04.2000) JP
特願2000-243207 2000年8月10日 (10.08.2000) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).

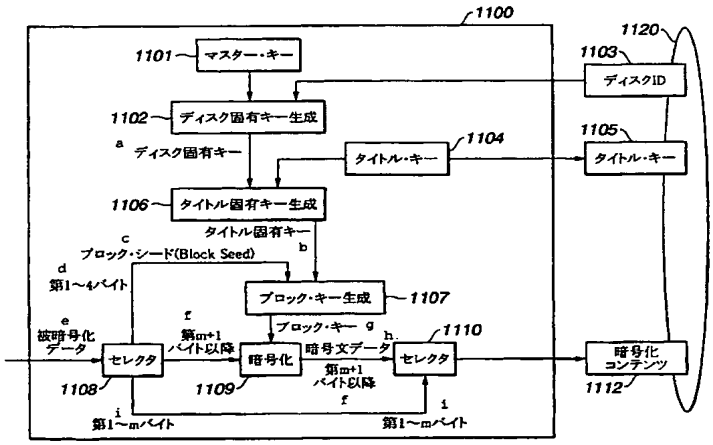
(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 浅野智之 (ASANO, Tomoyuki) [JP/JP]. 大澤義知 (OSAWA, Yoshitomo) [JP/JP]. 加藤元樹 (KATO, Motoki) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 小池 晃, 外 (KOIKE, Akira et al.); 〒105-0001 東京都港区虎ノ門二丁目6番4号 第11森ビル Tokyo (JP).

[続葉有]

(54) Title: INFORMATION RECORDING/REPRODUCING APPARATUS AND METHOD

(54) 発明の名称: 情報記録／再生装置及び方法



1101...MASTER KEY
1102...CREATION OF DISK UNIQUE KEY
a...DISK UNIQUE KEY
1104...TITLE KEY
1106...CREATION OF TITTLE UNIQUE KEY
b...TITLE UNIQUE KEY
c...BLOCK SEED
d...FIRST TO FOURTH BYTES
1107...CREATION OF BLOCK KEY
e...DATA TO BE CIPHERED
1108...SELECTOR
f...(m+1)-TH AND LATER BYTES
1109...CIPHERING
g...BLOCK KEY
h...CIPHERED TEXT DATA
1110...SELECTOR
i...FIRST TO m-TH BYTES
1103...DISK ID
1105...TITLE KEY
1112...CIPHERED CONTENT

(57) Abstract: A block key for ciphering block data by using ATS added depending on the arrival time of a transport packet constituting a transport stream is created. Since the ATS is random data depending on the time, a unique key different with block can be created, thereby enhancing the strength against cipher analysis. The block key is created by combining the ATS and keys unique to the device and the recording medium such as the master key, disk unique key, and title unique key. Since the block key is created using the ATS, no areas on the recording medium for storage of a ciphering key for each block is required.

WO 01/76127 A1

[続葉有]

(81) 指定国 (国内): AU, CN, ID, IN, KR, MX, RU, SG, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

添付公開書類:
— 国際調査報告書

(57) 要約:

トランスポートストリームを構成するランスポートパケットの着信時刻に応じて付加されるＡＴＳを用いてブロック・データを暗号化するブロックキーを生成する。ＡＴＳは時刻に応じたランダムなデータであるので、ブロック毎に異なる固有キーを生成でき、暗号解析に対する強度が高まる。ブロックキーは、ＡＴＳと、マスターキー、ディスク固有キー、タイトル固有キー等、デバイス、記録媒体に固有の鍵を組み合わせて生成する。ＡＴＳを用いてブロックキーを生成することにより、ブロック毎の暗号化鍵を格納するための記録媒体上の領域が不要となる。

明細書

情報記録／再生装置及び方法

技術分野

本発明は、情報記録装置、情報再生装置、情報記録方法、情報再生方法及び情報記録媒体、並びにプログラム提供媒体に関し、特に、データ記録再生可能な記録媒体に対するデータ書き込み、データ再生処理における違法コピーを防止することを可能とした情報記録装置、情報再生装置、情報記録方法、情報再生方法、及び情報記録媒体、並びにプログラム提供媒体に関する。

背景技術

ディジタル信号処理技術の進歩、発展に伴い、近年においては、情報を、ディジタル的に記録する記録装置や記録媒体が普及しつつある。このようなディジタル記録装置及び記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにディジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通することになると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなディジタルデータの不正なコピーを防ぐため、ディジタル記録装置及び記録媒体に違法なコピーを防止するための様々な仕組み（システム）が導入されている。

例えば、ＭＤ（ミニディスク）（ＭＤは商標）装置において、違法なコピーを防止する方法として、ＳＣＭＳ(Serial Copy Management System)が採用されている。ＳＣＭＳは、データ再生側において、オーディオデータとともにＳＣＭＳ信号をディジタルインタフェース（ＤＩＦ）から出力し、データ記録側において、

再生側からのＳＣＭＳ信号に基づいて、再生側からのオーディオデータの記録を制御することにより違法なコピーを防止するシステムである。

具体的にはＳＣＭＳ信号は、オーディオデータが、何度でもコピーが許容されるコピーフリー（copy free）のデータであるか、１度だけコピーが許されている（copy once allowed）データであるか、又はコピーが禁止されている（copy prohibited）データであるかを表す信号である。データ記録側において、ＤＩＦからオーディオデータを受信すると、そのオーディオデータとともに送信されるＳＣＭＳ信号を検出する。そして、ＳＣＭＳ信号が、コピーフリー（copy free）となっている場合には、オーディオデータをＳＣＭＳ信号とともにミニディスクに記録する。また、ＳＣＭＳ信号が、コピーを１度のみ許可（copy once allowed）となっている場合には、ＳＣＭＳ信号をコピー禁止（copy prohibited）に変更して、オーディオデータとともに、ミニディスクに記録する。さらに、ＳＣＭＳ信号が、コピー禁止（copy prohibited）となっている場合には、オーディオデータの記録を行わない。このようなＳＣＭＳを使用した制御を行うことで、ミニディスク装置では、ＳＣＭＳによって、著作権を有するオーディオデータが、違法にコピーされるのを防止するようになっている。

しかしながら、ＳＣＭＳは上述のようにＳＣＭＳ信号に基づいて再生側からのオーディオデータの記録を制御する構成をデータを記録する機器自体が有していることが前提であるため、ＳＣＭＳの制御を実行する構成を持たないミニディスク装置が製造された場合には、対処するのが困難となる。そこで、例えば、ＤＶＤプレーヤでは、コンテンツ・スクランブルシステムを採用することにより、著作権を有するデータの違法コピーを防止する構成となっている。

コンテンツ・スクランブルシステムでは、ＤＶＤ－ＲＯＭ(Read Only Memory)に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いるキー（復号鍵）が、ライセンスを受けたＤＶＤプレーヤに与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたＤＶＤプレーヤに対して与えられる。従って、ライセンスを受けたＤＶＤプレーヤでは、与えられたキーを利用して、ＤＶＤ－ＲＯＭに記録された暗号化データを復号することにより、ＤＶＤ－ＲＯＭから画

像や音声を再生することができる。

一方、ライセンスを受けていないＤＶＤプレーヤは、暗号化されたデータを復号するためのキーを有していないため、ＤＶＤ－ＲＯＭに記録された暗号化データの復号を行うことができない。このように、コンテンツ・スクランブルシステム構成では、ライセンス時に要求される条件を満たしていないＤＶＤプレーヤは、ディジタルデータを記録したＤＶＤ－ＲＯＭの再生を行えないことになり、不正コピーが防止されるようになっている。

しかしながら、ＤＶＤ－ＲＯＭで採用されているコンテンツ・スクランブルシステムは、ユーザによるデータの書き込みが不可能な記録媒体（以下、適宜、ＲＯＭメディアという）を対象としており、ユーザによるデータの書き込みが可能な記録媒体（以下、適宜、ＲＡＭメディアという）への適用については考慮されていない。

即ち、ＲＯＭメディアに記録されたデータが暗号化されていても、その暗号化されたデータを、そのまま全部、ＲＡＭメディアにコピーした場合には、ライセンスを受けた正当な装置で再生可能な、いわゆる海賊版を作成することができてしまう。

そこで、本出願人は、先の特許出願、特開平１１－２２４４６１号公報（特願平１０－２５３１０号）において、個々の記録媒体を識別するための情報（以下、媒体識別情報と記述する）を、他のデータとともに記録媒体に記録し、この媒体識別情報のライセンスを受けた装置であることを条件として、その条件が満たされた場合にのみ記録媒体の媒体識別情報へのアクセスが可能となる構成を提案した。

この方法では、記録媒体上のデータは、媒体識別情報とライセンスを受けることにより得られる秘密キー（マスターキー）により暗号化され、ライセンスを受けていない装置が、この暗号化されたデータを読み出したとしても、意味のあるデータを得ることができないようになっている。なお、装置はライセンスを受ける際、不正な複製（違法コピー）ができないように、その動作が規定される。

ライセンスを受けていない装置は、媒体識別情報にアクセスできず、また、媒体識別情報は個々の媒体毎に個別の値となっているため、ライセンスを受けてい

ない装置が、記録媒体に記録されている、暗号化されたデータのすべてを新たな記録媒体に複製したとしても、そのようにして作成された記録媒体に記録されたデータは、ライセンスを受けていない装置は勿論、ライセンスを受けた装置においても、正しく復号することができないから、実質的に、違法コピーが防止されることになる。

ところで、特開平１１－２２４４６１号公報（特願平１０－２５３１０号）において開示している構成は、ディスクに記録する画像、音声、プログラム等のコンテンツデータを各セクタ毎に個別の鍵セクタキーを用いて暗号化する構成としている。

これは、１つの暗号鍵で大量のデータを暗号化すると、媒体上に格納された暗号文と、何らかの手段で攻撃者が入手した平文の組を用いて、差分攻撃や線形攻撃などの暗号攻撃の手法により、暗号鍵が露呈しやすくなるという課題に対処するためである。上記の出願ではセクタという決まった大きさ毎に暗号鍵を変えることにより、１つの暗号鍵で処理するデータの量を小さく押さえて暗号鍵の解読を困難にすることができる。さらに、万が一鍵が解読された場合においても復号可能なデータ量を少なくすることができる。

しかしながら、上記公報に記載の例では、コンテンツの暗号化に使用したセクタ毎の暗号鍵（セクタキー）をさらに上位の鍵で暗号化して、記録媒体のセクタヘッダに格納している。このため、セクタヘッダに暗号化したセクタキーを格納するだけの領域が必要になり、また、コンテンツの記録、再生時に、メインデータ部だけでなく、セクタヘッダにアクセスをして暗号化セクタキーの書き込み（記録時）もしくは読出し（再生時）を行わなければならない。

発明の開示

本発明は、上述のような従来技術の問題点を解決することを目的とするものであり、ブロックデータの暗号化処理を異なる鍵で実行可能として暗号解析に対する強度を高めることができる構成とするとともに、暗号鍵の格納領域をディスク上に新たに設ける必要を排除してデータ領域を狭めることのない構成を実現する

情報記録装置、情報再生装置、情報記録方法、情報再生方法、及び情報記録媒体、並びにプログラム提供媒体を提供する。

より、具体的には、本発明は、データを構成するトランスポートストリームに含まれる各パケットの着信時刻に応じたランダム性のあるデータとして構成されるＡＴＳを用いてブロック・データを暗号化するブロックキーを生成する構成としてブロック毎に異なる固有キーを生成することで、暗号解析に対する強度を高め、また、ＡＴＳを用いてブロックキーを生成する構成とすることにより、各ブロック毎の暗号化鍵を格納するための記録媒体上の領域を不要としてメインデータ領域を有効に使用可能とする情報記録装置、情報再生装置、情報記録方法、情報再生方法、及び情報記録媒体、並びにプログラム提供媒体を提供することを目的とする。

上述した目的を達成する本発明の第１の側面は、記録媒体に情報を記録する情報記録装置において、間欠的なトランスポートパケットからなるトランスポートストリームを構成する各パケットに受信時刻情報（ＡＴＳ）を付加するトランスポート・ストリーム処理手段と、前記受信時刻情報（ＡＴＳ）の付加された１以上のパケットからなるブロックデータに対する暗号処理用のブロックキーを前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の暗号処理を実行する暗号処理手段と、を有し、前記暗号処理手段によって暗号化したデータを前記記録媒体に記録する構成としたことを特徴とする情報記録装置にある。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記ブロックデータを構成する複数のトランスポートパケットの先頭のトランスポートパケットに付加された受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードに基づいて、前記ブロックデータに対する暗号処理用のブロックキーを生成する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基

づいてタイトル固有キーを生成し、該タイトル固有キーと前記ブロックシードに基づいてブロックキーを生成する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとを生成して前記記録媒体に格納する処理を実行する構成を有することを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記ブロックシードは、前記受信時刻情報（ＡＴＳ）の他にコピー制御情報を含むデータであることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記ブロックデータの暗号処理において、該ブロックデータのブロックシードを含む先頭領域データ以外のブロックデータ構成データのみを前記ブロックキーにより暗号化する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーを暗号関数の鍵とし、前記ブロックシードを前記暗号関数に入力して暗号化した結果をブロックキーとして出力する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーと、前記ブロックシードとを一方向関数に入力して暗号化した結果をブロックキーとして出力する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、該暗号処理手段を構成するＬＳＩに格納されたＬＳＩキー、前記情報記録装置に格納されたデバイスキー、前記記録媒体に格納されたメディアキー、前記記録媒体のドライブ装置に格納されたドライブキーのいずれか、又はこれら各キーの組

合わせに基づいてデバイス固有キーを生成し、生成したデバイス固有キーと前記ブロックシードとに基づいて前記ブロックデータに対する暗号処理用のブロックキーを生成する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記ブロックデータに対するブロックキーによる暗号処理をＤＥＳアルゴリズムに従って実行する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、前記トランスポートストリームを構成する各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に対する記録実行の可否を制御する構成を有することを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)を識別し、該ＥＭＩに基づいて記録媒体に対する記録実行の可否を制御する構成を有することを特徴とする。

さらに、本発明の第２の側面は、記録媒体から情報を再生する情報再生装置において、前記記録媒体に記録された暗号データを復号する暗号処理手段であり、複数のトランスポートパケットの各々に受信時刻情報（ＡＴＳ）を付加したブロックデータの暗号化データに対する復号処理用のブロックキーを前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の復号処理を実行する暗号処理手段と、前記暗号処理手段において復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報（ＡＴＳ）に基づいてデータ出力制御を実行するトランスポート・ストリーム処理手段と、を有することを特徴とする情報再生装置にある。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記ブロックデータを構成する複数のトランスポートパケットの先頭のトランスポートパケットに付加された受信時刻情報（ＡＴＳ）を含むブロックデータ固有

の付加情報であるブロックシードに基づいて、前記ブロックデータに対する復号処理用のブロックキーを生成する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、該タイトル固有キーと前記ブロックシードに基づいてブロックキーを生成する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記ブロックシードは、前記受信時刻情報（ＡＴＳ）の他にコピー制御情報を含むデータであることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記ブロックデータの復号処理において、該ブロックデータのブロックシードを含む先頭領域データ以外のブロックデータ構成データのみを前記ブロックキーにより復号する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーを暗号関数の鍵とし、前記ブロックシードを前記暗号関数に入力して暗号化した結果をブロックキーとして出力する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーと、前記ブロックシードとを一方向関数に入力して暗号化した結果をブロックキーとして出力する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、該暗号処理手段を構成するＬＳＩに格納されたＬＳＩキー、前記情報記録装置に格納されたデバイスキー、前記記録媒体に格納されたメディアキー、前記記録媒

体のドライブ装置に格納されたドライブキーのいずれか、又はこれら各キーの組合わせに基づいてデバイス固有キーを生成し、生成したデバイス固有キーと前記ブロックシードとに基づいて前記ブロックデータに対する復号処理用のブロックキーを生成する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記ブロックデータに対するブロックキーによる復号処理をＤＥＳアルゴリズムに従って実行する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記情報再生装置は、記録媒体からの再生対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、前記トランスポートストリームを構成する各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて再生実行の可否を制御する構成を有することを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記情報再生装置は、記録媒体からの再生対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)を識別し、該ＥＭＩに基づいて再生実行の可否を制御する構成を有することを特徴とする。

さらに、本発明の第３の側面は、記録媒体に情報を記録する情報記録方法において、トランスポートパケットからなるトランスポートストリームを構成する各パケットに受信時刻情報（ＡＴＳ）を付加するトランスポート・ストリーム処理ステップと、前記受信時刻情報（ＡＴＳ）の付加された１以上のパケットからなるブロックデータに対する暗号処理用のブロックキーを前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の暗号処理を実行する暗号処理ステップと、を有し、前記暗号処理ステップによって暗号化したデータを前記記録媒体に記録することを特徴とする情報記録方法にある。

さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、前記ブロックデータを構成する複数のトランスポートパケットの先頭のトランスポートパケットに付加された受信時刻情報（ＡＴＳ）を含むブロックデータ

固有の付加情報であるブロックシードに基づいて、前記ブロックデータに対する暗号処理用のブロックキーを生成することを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、該タイトル固有キーと前記ブロックシードに基づいてブロックキーを生成することを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとを生成して前記記録媒体に格納する処理を実行する識別子生成ステップを有することを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、前記ブロックデータの暗号処理において、該ブロックデータのブロックシードを含む先頭領域データ以外のブロックデータ構成データのみを前記ブロックキーにより暗号化することを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーを暗号関数の鍵とし、前記ブロックシードを前記暗号関数に入力して暗号化した結果をブロックキーとして出力することを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーと、前記ブロックシードとを一方向関数に入力して暗号化した結果をブロックキーとして出力することを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、暗号処理手段を構成するＬＳＩに格納されたＬＳＩキー、情報記録装置に格

納されたデバイスキー、前記記録媒体に格納されたメディアキー、前記記録媒体のドライブ装置に格納されたドライブキーのいずれか、又はこれら各キーの組合わせに基づいてデバイス固有キーを生成し、生成したデバイス固有キーと前記ブロックシードとに基づいて前記ブロックデータに対する暗号処理用のブロックキーを生成することを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、前記ブロックデータに対するブロックキーによる暗号処理をＤＥＳアルゴリズムに従って実行することを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、前記トランスポートストリームを構成する各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に対する記録実行の可否を制御するコピー制御ステップを有することを特徴とする。

さらに、本発明の情報記録方法の一実施態様において、コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)を識別し、該ＥＭＩに基づいて記録媒体に対する記録実行の可否を制御するコピー制御ステップを有することを特徴とする。

さらに、本発明の第４の側面は、記録媒体から情報を再生する情報再生方法において、複数のトランスポートパケットの各々に受信時刻情報（ＡＴＳ）を付加したブロックデータの暗号化データに対する復号処理用のブロックキーを前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の復号処理を実行する復号処理ステップと、前記暗号処理ステップにおいて復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報（ＡＴＳ）に基づいてデータ出力制御を実行するトランスポート・ストリーム処理ステップと、を有することを特徴とする情報再生方法にある。

さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、前記ブロックデータを構成する複数のトランスポートパケットの先頭のトランスポートパケットに付加された受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードに基づいて、前記ブロックデータに対する

復号処理用のブロックキーを生成することを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、該タイトル固有キーと前記ブロックシードに基づいてブロックキーを生成することを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、前記ブロックデータの復号処理において、該ブロックデータのブロックシードを含む先頭領域データ以外のブロックデータ構成データのみを前記ブロックキーにより復号することを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーを暗号関数の鍵とし、前記ブロックシードを前記暗号関数に入力して暗号化した結果をブロックキーとして出力することを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーと、前記ブロックシードとを一方向関数に入力して暗号化した結果をブロックキーとして出力することを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、暗号処理手段を構成するＬＳＩに格納されたＬＳＩキー、情報記録装置に格納されたデバイスキー、前記記録媒体に格納されたメディアキー、前記記録媒体のドライブ装置に格納されたドライブキーのいずれか、又はこれら各キーの組合わせに基づいてデバイス固有キーを生成し、生成したデバイス固有キーと前記ブロックシードとに基づいて前記ブロックデータに対する復号処理用のブロックキーを生成することを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、前記ブロックデータに対するブロックキーによる復号処理をＤＥＳアルゴリズムに従って実行することを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、前記トランスポートストリームを構成する各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体からの情報再生実行の可否を制御するコピー制御ステップを有することを特徴とする。

さらに、本発明の情報再生方法の一実施態様において、コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)を識別し、該ＥＭＩに基づいて記録媒体からの情報再生実行の可否を制御するコピー制御ステップを有することを特徴とする。

さらに、本発明の第５の側面は、トランスポートストリームを構成する各パケットに受信時刻情報（ＡＴＳ）を付加した１以上のパケットからなるブロックデータの暗号化鍵として使用されるブロックキーの生成情報となる受信時刻情報（ＡＴＳ）を含むブロックシードを有する非暗号化データ部と、前記ブロックキーにより暗号化された暗号化データ部と、を構成要素とするブロックデータを記録したことを特徴とする記録媒体にある。

さらに、本発明の第６の側面は、記録媒体に情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、間欠的なトランスポートパケットからなるトランスポートストリームを構成する各パケットに受信時刻情報（ＡＴＳ）を付加するトランスポート・ストリーム処理ステップと、前記受信時刻情報（ＡＴＳ）の付加された１以上のパケットからなるブロックデータに対する暗号処理用のブロックキーを前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の暗号処理を実行する暗号処理ステップと、を有することを特徴とするプログラム提供媒体にある。

さらに、本発明の第７の側面は、記録媒体から情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供する

プログラム提供媒体であって、前記コンピュータ・プログラムは、複数のトランスポートパケットの各々に受信時刻情報（ＡＴＳ）を付加したブロックデータの暗号化データに対する復号処理用のブロックキーを前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の復号処理を実行する復号処理ステップと、前記暗号処理ステップにおいて復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報（ＡＴＳ）に基づいてデータ出力制御を実行するトランスポート・ストリーム処理ステップと、を有することを特徴とするプログラム提供媒体にある。

本発明においては、記録媒体に記録するコンテンツの形式をＭＰＥＧ２ ＴＳパケット（ｐａｃｋｅｔ）とし、このパケットを記録装置が受信した時刻情報であるＡＴＳを付加して記録する。ＡＴＳは２４乃至３２ビットのデータであり、ある程度のランダム性がある。ここで、ＡＴＳはArrival Time Stamp（着信時刻スタンプ）の略である。

記録媒体のひとつのブロック（セクタ）には、ＡＴＳを付加したＴＳパケットをＸ個記録することにし、その第１番目のＴＳパケットに付加されたＡＴＳを用いてそのブロックのデータを暗号化するブロックキーを生成する。

このようにすることにより、各ブロック毎に固有の鍵を用いて暗号化することができ、また鍵を格納する特別な領域も不要となり、記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなる。

さらに、ＴＳパケットにＡＴＳだけでなくコピー制限情報(ＣＣＩ：Copy Control Information)も付加して記録し、ＡＴＳとＣＣＩを用いてブロックキーを生成するようにすることも可能である。

なお、本発明の第６及び第７の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、ＣＤやＦＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピ

ュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

図面の簡単な説明

図１は、本発明の情報記録再生装置の構成例（その１）を示すブロック図である。

図２は、本発明の情報記録再生装置の構成例（その２）を示すブロック図である。

図３Ａ及び図３Ｂは、本発明の情報記録再生装置のデータ記録処理フローを示す図である。

図４Ａ及び図４Ｂは、本発明の情報記録再生装置のデータ再生処理フローを示す図である。

図５は、本発明の情報記録再生装置において処理されるデータフォーマットを説明する図である。

図６は、本発明の情報記録再生装置におけるトランスポート・ストリーム（ＴＳ）処理手段の構成を示すブロック図である。

図７Ａ～図７Ｃは、本発明の情報記録再生装置において処理されるトランスポート・ストリームの構成を説明する図である。

図８は、本発明の情報記録再生装置におけるトランスポート・ストリーム（ＴＳ）処理手段の構成を示すブロック図である。

図９は、本発明の情報記録再生装置におけるトランスポート・ストリーム（ＴＳ）処理手段の構成を示すブロック図である。

図１０は、本発明の情報記録再生装置において処理されるブロックデータの付

加情報としてのブロック・データの構成例を示す図である。

図１１は、本発明の情報記録再生装置において、データ互換性の要請されるシステムにおけるデータ記録処理時の暗号化処理を説明するブロック図（その１）である。

図１２は、本発明の情報記録再生装置において、データ互換性の要請されるシステムにおけるデータ記録処理時の暗号化処理を説明するブロック図（その２）である。

図１３は、本発明の情報記録再生装置において、データ互換性の要請されるシステムにおけるデータ記録処理時の暗号化処理を説明するフローチャートである。

図１４は、本発明の情報記録再生装置におけるブロック・キーの生成方法を説明する図である。

図１５は、本発明の情報記録再生装置において、データ互換性の要請されるシステムにおけるデータ再生処理時の復号処理を説明するブロック図である。

図１６は、本発明の情報記録再生装置において、データ互換性の要請されるシステムにおけるデータ再生処理時の復号処理を説明するフローチャートである。

図１７は、本発明の情報記録再生装置において、データ互換性の要請されないシステムにおけるデータ記録処理時の暗号化処理を説明するブロック図である。

図１８は、本発明の情報記録再生装置において、データ互換性の要請されないシステムにおけるデータ記録処理時の暗号化処理を説明するフローチャートである。

図１９は、本発明の情報記録再生装置において、データ互換性の要請されないシステムにおけるデバイス固有キー生成処理例（その１）を説明するブロック図である。

図２０は、本発明の情報記録再生装置において、データ互換性の要請されないシステムにおけるデバイス固有キー生成処理例（その２）を説明するブロック図である。

図２１は、本発明の情報記録再生装置において、データ互換性の要請されないシステムにおけるデータ再生処理時の復号処理を説明するブロック図である。

図２２は、本発明の情報記録再生装置において、データ互換性の要請されない

システムにおけるデータ再生処理時の復号処理を説明するフローチャートである。

図２３は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ記録処理時の暗号化処理を説明するブロック図（その１）である。

図２４は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ記録処理時の暗号化処理を説明するブロック図（その２）である。

図２５は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ記録処理を説明するフローチャートである。

図２６は、本発明の情報記録再生装置におけるディスク固有キーの生成例を説明する図である。

図２７は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるタイトル固有キーの生成処理フローを示す図である。

図２８は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ記録時のタイトル固有キーの生成処理例を示す図である。

図２９は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ再生処理時の復号処理を説明するブロック図である。

図３０は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ再生処理を説明するフローチャートである。

図３１は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ再生処理における再生可能制判定処理の詳細を示すフローチャートである。

図３２は、本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ最盛時のタイトル固有キーの生成処理フローを示す図である。

図３３Ａ及び図３３Ｂは、本発明の情報記録再生装置におけるデータ記録処理時のコピー制御処理を説明するフローチャートである。

図３４Ａ及び図３４Ｂは、本発明の情報記録再生装置におけるデータ再生処理時のコピー制御処理を説明するフローチャートである。

図３５は、本発明の情報記録再生装置において、データ処理をソフトウェアによって実行する場合の処理手段構成を示したブロック図である。

発明を実施するための最良の形態

[システム構成]

図１は、本発明を適用した記録再生装置１００の一実施例形態の構成を示すブロック図である。記録再生装置１００は、入出力Ｉ／Ｆ(Interface)１２０、ＭＰＥＧ(Moving Picture Experts Group)コーデック１３０、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を備えた入出力Ｉ／Ｆ(Interface)１４０、暗号処理手段１５０、ＲＯＭ (Read Only Memory) １６０、ＣＰＵ(Central Processing Unit)１７０、メモリ１８０、記録媒体１９５のドライブ１９０、さらにトランスポート・ストリーム処理手段（ＴＳ処理手段）３００を有し、これらはバス１１０によって相互に接続されている。

入出力Ｉ／Ｆ１２０は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するディジタル信号を受信し、バス１１０上に出力するとともに、バス１１０上のディジタル信号を受信し、外部に出力する。ＭＰＥＧコーデック１３０は、バス１１０を介して供給されるＭＰＥＧ符号化されたデータを、ＭＰＥＧデコードし、入出力Ｉ／Ｆ１４０に出力するとともに、入出力Ｉ／Ｆ１４０から供給されるディジタル信号をＭＰＥＧエンコードしてバス１１０上に出力する。入出力Ｉ／Ｆ１４０は、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を内蔵している。入出力Ｉ／Ｆ１４０は、外部から供給されるコンテンツとしてのアナログ信号を受信し、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＡ／Ｄ(Analog Digital)変換することで、ディジタル信号として、ＭＰＥＧコーデック１３０に出力するとともに、ＭＰＥＧコーデック１３０からのディジタル信号を、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＤ／Ａ(Digital Analog)変換することで、アナログ信号として、外部に出力する。

暗号処理手段１５０は、例えば、１チップのＬＳＩ(Large Scale Integrated Curcuit)で構成され、バス１１０を介して供給されるコンテンツとしてのディジタル信号を暗号化し、又は復号し、バス１１０上に出力する構成を持つ。なお、暗号処理手段１５０は１チップＬＳＩに限らず、各種のソフトウェア又はハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構

成による処理手段としての構成については後段で説明する。

ＲＯＭ１６０は、例えば、記録再生装置毎に固有の、あるいは、複数の記録再生装置のグループ毎に固有のデバイスキーを記憶している。ＣＰＵ１７０は、メモリ１８０に記憶されたプログラムを実行することで、ＭＰＥＧコーデック１３０や暗号処理手段１５０等を制御する。メモリ１８０は、例えば、不揮発性メモリで、ＣＰＵ１７０が実行するプログラムや、ＣＰＵ１７０の動作上必要なデータを記憶する。ドライブ１９０は、ディジタルデータを記録再生可能な記録媒体１９５を駆動することにより、記録媒体１９５からディジタルデータを読み出し（再生し）、バス１１０上に出力するとともに、バス１１０を介して供給されるディジタルデータを、記録媒体１９５に供給して記録させる。なお、プログラムをＲＯＭ１６０に、デバイスキーをメモリ１８０に記憶するように構成してもよい。

記録媒体１９５は、例えば、ＤＶＤ、ＣＤ等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはＲＡＭ等の半導体メモリ等のディジタルデータの記憶可能な媒体であり、本実施の形態では、ドライブ１９０に対して着脱可能な構成であるとする。但し、記録媒体１９５は、記録再生装置１００に内蔵する構成としてもよい。

トランスポート・ストリーム処理手段（ＴＳ処理手段）３００は、後段において図６以下を用いて詳細に説明するが、例えば複数のＴＶプログラム（コンテンツ）が多重化されたトランスポートストリームから特定のプログラム（コンテンツ）に対応するトランスポートパケットを取り出して、取り出したトランスポートストリームの出現タイミング情報を各パケットとともに記録媒体１９５に格納するためのデータ処理及び、記録媒体１９５からの再生処理時の出現タイミング制御処理を行う。

トランスポートストリームには、各トランスポートパケットの出現タイミング情報としてのＡＴＳ（Arrival Time Stamp：着信時刻スタンプ）が設定されており、このタイミングはＭＰＥＧ２システムズで規定されている仮想的なデコーダであるＴ－ＳＴＤ(Transport stream System Target Decoder)を破綻させないように符号化時に決定され、トランスポートストリームの再生時には、各トラ

ンスポートパケットに付加されたＡＴＳによって出現タイミングを制御する。トランスポート・ストリーム処理手段（ＴＳ処理手段）３００は、これらの制御を実行する。例えば、トランスポートパケットを記録媒体に記録する場合には、各パケットの間隔を詰めたソースパケットとして記録するが、各トランスポートパケットの出現タイミングを併せて記録媒体に保存することにより、再生時に各パケットの出力タイミングを制御することが可能となる。トランスポート・ストリーム処理手段（ＴＳ処理手段）３００は、ＤＶＤ等の記録媒体１９５へのデータ記録時に、各トランスポートパケットの入力タイミングを表すＡＴＳ（Arrival Time Stamp：着信時刻スタンプ）を付加して記録する。

本発明の記録再生装置１００は、上述のＡＴＳの付加されたトランスポートストリームによって構成されるコンテンツについて、暗号処理手段１５０において暗号化処理を実行し、暗号化処理のなされたコンテンツを記録媒体１９５に格納する。さらに、暗号処理手段１５０は、記録媒体１９５に格納された暗号化コンテンツの復号処理を実行する。これらの処理の詳細については、後段で説明する。

なお、図１に示す暗号処理手段１５０、ＴＳ処理手段３００は、理解を容易にするため、別ブロックとして示してあるが、両機能を実行する１つのワンチップＬＳＩとして構成してもよく、また、両機能をソフトウェア又はハードウェアを組み合わせた構成によって実現する構成としてもよい。

本発明の記録再生装置の構成例としては図１に示す構成の他に図２に示す構成が可能である。図２に示す記録再生装置２００では、記録媒体２０５はドライブ装置としての記録媒体インタフェース（Ｉ／Ｆ）２１０から着脱が可能であり、この記録媒体２０５を別の記録再生装置に装着してもデータの読出し、書き込みが可能な構成としたものである。このように、記録媒体１９５が複数の記録再生装置において使用可能な構成を持つ図２のような記録再生装置においては記録再生装置毎に固有のデバイスキーを持つのではなく、複数の記録再生装置に共通な鍵、即ちシステム全体で共通な鍵をメモリ１８０に格納する構成とする。

［データ記録処理及びデータ再生処理］

次に、図１あるいは図２の記録再生装置における記録媒体に対するデータ記録処理及び記録媒体からのデータ再生処理について、図３及び図４のフローチャー

トを参照して説明する。外部からのディジタル信号のコンテンツを、記録媒体１９５に記録する場合においては、図３（Ａ）のフローチャートに従った記録処理が行われる。即ち、ディジタル信号のコンテンツ（ディジタルコンテンツ）が、例えば、IEEE(Institute of Electrical and Electronics Engineers)1394シリアルバス等を介して、入出力Ｉ／Ｆ１２０に供給されると、ステップＳ３０１において、入出力Ｉ／Ｆ１２０は、供給されるディジタルコンテンツを受信し、バス１１０を介して、ＴＳ処理手段３００に出力する。

ＴＳ処理手段３００は、ステップＳ３０２において、トランスポートストリームを構成する各トランスポートパケットにＡＴＳを付加したブロックデータを生成して、バス１１０を介して、暗号処理手段１５０に出力する。

暗号処理手段１５０は、ステップＳ３０３において、受信したディジタルコンテンツに対する暗号化処理を実行し、その結果得られる暗号化コンテンツを、バス１１０を介して、ドライブ１９０、あるいは記録媒体Ｉ／Ｆ２１０に出力する。暗号化コンテンツは、ドライブ１９０、あるいは記録媒体Ｉ／Ｆ２１０を介して記録媒体１９５に記録（Ｓ３０４）され、記録処理を終了する。なお、暗号処理手段１５０における暗号処理については後段で説明する。

なお、IEEE1394シリアルバスを介して接続した装置相互間で、ディジタルコンテンツを伝送するときの、ディジタルコンテンツを保護するための規格として、本特許出願人であるソニー株式会社を含む５社によって、５ＣＤＴＣＰ(Five Company Digital Transmission Content Protection)（以下、適宜、ＤＴＣＰという）が定められているが、このＤＴＣＰでは、コピーフリーでないディジタルコンテンツを装置相互間で伝送する場合、データ伝送に先立って、送信側と受信側が、コピーを制御するためのコピー制御情報を正しく取り扱えるかどうかの認証を相互に行い、その後、送信側において、ディジタルコンテンツを暗号化して伝送し、受信側において、その暗号化されたディジタルコンテンツ（暗号化コンテンツ）を復号するようになっている。

このＤＴＣＰに規格に基づくデータ送受信においては、データ受信側の入出力Ｉ／Ｆ１２０は、ステップＳ３０１で、IEEE1394シリアルバスを介して暗号化コンテンツを受信し、その暗号化コンテンツを、ＤＴＣＰに規格に準拠して復号し、

平文のコンテンツとして、その後、暗号処理手段１５０に出力する。

ＤＴＣＰによるディジタルコンテンツの暗号化は、時間変化するキーを生成し、そのキーを用いて行われる。暗号化されたディジタルコンテンツは、その暗号化に用いたキーを含めて、IEEE1394シリアルバス上を伝送され、受信側では、暗号化されたディジタルコンテンツを、そこに含まれるキーを用いて復号する。

なお、ＤＴＣＰによれば、正確には、キーの初期値と、ディジタルコンテンツの暗号化に用いるキーの変更タイミングを表すフラグとが、暗号化コンテンツに含められる。そして、受信側では、その暗号化コンテンツに含まれるキーの初期値を、やはり、その暗号化コンテンツに含まれるフラグのタイミングで変更していくことで、暗号化に用いられたキーが生成され、暗号化コンテンツが復号される。但し、ここでは、暗号化コンテンツに、その復号を行うためのキーが含まれていると等価であると考えても差し支えないため、以下では、そのように考えるものとする。ここで、ＤＴＣＰについては、例えば、http://www.dtcp.comのURL(Uniform Resource Locator)で特定されるＷｅｂページにおいて、インフォメイショナルバージョン(Informational Version)の取得が可能である。

次に、外部からのアナログ信号のコンテンツを、記録媒体１９５に記録する場合の処理について、図３（Ｂ）のフローチャートに従って説明する。アナログ信号のコンテンツ（アナログコンテンツ）が、入出力Ｉ／Ｆ１４０に供給されると、入出力Ｉ／Ｆ１４０は、ステップＳ３２１において、そのアナログコンテンツを受信し、ステップＳ３２２に進み、内蔵するＡ／Ｄ，Ｄ／Ａコンバータ１４１でＡ／Ｄ変換して、ディジタル信号のコンテンツ（ディジタルコンテンツ）とする。

このディジタルコンテンツは、ＭＰＥＧコーデック１３０に供給され、ステップＳ３２３において、ＭＰＥＧエンコード、即ちＭＰＥＧ圧縮による符号化処理が実行され、バス１１０を介して、暗号処理手段１５０に供給される。

以下、ステップＳＳ３２４、Ｓ３２５、Ｓ３２６において、図３（Ａ）のステップＳ３０２、Ｓ３０３における処理と同様の処理が行われる。即ち、ＴＳ処理手段３００によるトランスポートパケットに対するＡＴＳ付加、暗号処理手段１５０における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体１９５に記録して、記録処理を終了する。

次に、記録媒体１９５に記録されたコンテンツを再生して、ディジタルコンテンツ、あるいはアナログコンテンツとして出力する処理について図４のフローに従って説明する。ディジタルコンテンツとして外部に出力する処理は図４（Ａ）のフローチャートに従った再生処理として実行される。即ち、まず最初に、ステップＳ４０１において、ドライブ１９０又は記録媒体Ｉ／Ｆ２１０によって、記録媒体１９５に記録された暗号化コンテンツが読み出され、バス１１０を介して、暗号処理手段１５０に出力される。

暗号処理手段１５０では、ステップＳ４０２において、ドライブ１９０又は記録媒体Ｉ／Ｆ２１０から供給される暗号化コンテンツが復号処理され、復号データがバス１１０を介して、ＴＳ処理手段３００に出力される。

ＴＳ処理手段３００は、ステップＳ４０３において、トランスポートストリームを構成する各トランスポートパケットのＡＴＳから出力タイミングを判定し、ＡＴＳに応じた制御を実行して、バス１１０を介して、入出力Ｉ／Ｆ１２０に供給する。入出力Ｉ／Ｆ１２０は、ＴＳ処理手段３００からのディジタルコンテンツを、外部に出力し、再生処理を終了する。なお、ＴＳ処理手段３００の処理、暗号処理手段１５０におけるディジタルコンテンツの復号処理については後述する。

なお、入出力Ｉ／Ｆ１２０は、ステップＳ４０４で、IEEE1394シリアルバスを介してディジタルコンテンツを出力する場合には、ＤＴＣＰの規格に準拠して、上述したように、相手の装置との間で認証を相互に行い、その後、ディジタルコンテンツを暗号化して伝送する。

記録媒体１９５に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図４（Ｂ）のフローチャートに従った再生処理が行われる。

即ち、ステップＳ４２１、Ｓ４２２、Ｓ４２３において、図４（Ａ）のステップＳ４０１、Ｓ４０２、Ｓ４０３における場合とそれぞれ同様の処理が行われ、これにより、暗号処理手段１５０において得られた復号されたディジタルコンテンツは、バス１１０を介して、ＭＰＥＧコーデック１３０に供給される。

ＭＰＥＧコーデック１３０では、ステップＳ４２４において、ディジタルコン

テンツがＭＰＥＧデコード、即ち伸長処理が実行され、入出力Ｉ／Ｆ１４０に供給される。入出力Ｉ／Ｆ１４０は、ステップＳ４２４において、ＭＰＥＧコーデック１３０でＭＰＥＧデコードされたディジタルコンテンツを、内蔵するＡ／Ｄ，Ｄ／Ａコンバータ１４１でＤ／Ａ変換（Ｓ４２５）して、アナログコンテンツとする。そして、ステップＳ４２６に進み、入出力Ｉ／Ｆ１４０は、そのアナログコンテンツを、外部に出力し、再生処理を終了する。

［データフォーマット］

次に、図５を用いて、本発明における記録媒体上のデータフォーマットを説明する。本発明における記録媒体上のデータの読み書きの最小単位をブロック(block)という名前で呼ぶ。１ブロックは、１９２＊Ｘ（エックス）バイト（例えばＸ＝３２）の大きさとなっている。

本発明では、ＭＰＥＧ２のＴＳ（トランスポート・ストリーム）パケット（１８８バイト）にＡＴＳを付加して１９２バイトとして、それをＸ個集めて１ブロックのデータとしている。ＡＴＳは２４乃至３２ビットの着信時刻を示すデータであり、先にも説明したようにArrival Time Stamp（着信時刻スタンプ）の略である。ＡＴＳは各パケットの着信時刻に応じたランダム性のあるデータとして構成される。記録媒体のひとつのブロック（セクタ）には、ＡＴＳを付加したＴＳ（トランスポート・ストリーム）パケットをＸ個記録する。本発明の構成では、トランスポートストリームを構成する各ブロックの第１番目のＴＳパケットに付加されたＡＴＳを用いてそのブロック（セクタ）のデータを暗号化するブロックキーを生成する。

ランダム性のあるＡＴＳを用いて暗号化用のブロックキーを生成することにより、ブロック毎に異なる固有キーが生成される。生成されたブロック固有キーを用いてブロック毎の暗号化処理を実行する。また、ＡＴＳを用いてブロックキーを生成する構成とすることにより、各ブロック毎の暗号化鍵を格納するための記録媒体上の領域が不要となり、メインデータ領域が有効に使用可能となる。さらに、データの記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなり、処理が効率的になる。

なお、図５に示すブロック・シード（Block Seed）は、ＡＴＳを含む付加情報

である。ブロック・シードは、さらにＡＴＳだけでなくコピー制限情報(ＣＣＩ：Copy Control Information)も付加した構成としてもよい。この場合、ＡＴＳとＣＣＩを用いてブロックキーを生成する構成とすることができる。

なお、本発明の構成においては、ＤＶＤ等の記録媒体上にデータを格納する場合、コンテンツの大部分のデータは暗号化されるが、図５の最下段に示すように、ブロックの先頭のｍ（例えば、ｍ＝８又は１６）バイトは暗号化されずに平文（Unencrypted data）のまま記録され、残りのデータ（ｍ＋１バイト以降）が暗号化される。これは暗号処理が８バイト単位としての処理であるために暗号処理データ長（Encrypted data）に制約が発生するためである。なお、もし暗号処理が８バイト単位でなく、例えば１バイト単位で行えるなら、ｍ＝４として、ブロックシード以外の部分をすべて暗号化してもよい。

［ＴＳ処理手段における処理］

ここで、ＡＴＳの機能について詳細に説明する。ＡＴＳは、先にも説明したように入力トランスポートストリーム中の各トランスポートパケットの出現タイミングを保存するために付加する着信時刻スタンプである。

即ち、例えば複数のＴＶプログラム（コンテンツ）が多重化されたトランスポートストリームの中から１つ又は幾つかのＴＶプログラム（コンテンツ）を取り出した時、その取り出したトランスポートストリームを構成するトランスポートパケットは、不規則な間隔で現れる（図７（Ａ）参照）。トランスポートストリームは、各トランスポートパケットの出現タイミングに重要な意味があり、このタイミングはＭＰＥＧ２システムズ(ISO/IEC 13818-1)で規定されている仮想的なデコーダであるＴ－ＳＴＤ(Transport stream System Target Decoder)を破綻させないように符号化時に決定される。

トランスポートストリームの再生時には、各トランスポートパケットに付加されたＡＴＳによって出現タイミングが制御される。従って、記録媒体にトランスポートパケットを記録する場合には、トランスポートパケットの入力タイミングを保存する必要があり、トランスポートパケットをＤＶＤ等の記録媒体に記録する時に、各トランスポートパケットの入力タイミングを表すＡＴＳを付加して記録する。

図６に、ディジタルインタフェース経由で入力されるトランスポートストリームをＤＶＤ等の記録媒体であるストレージメディアに記録する時のＴＳ処理手段３００において実行する処理を説明するブロック図を示す。端子６００からは、ディジタル放送等のディジタルデータとしてトランスポートストリームが入力される。図１又は図２においては、入出力Ｉ／Ｆ１２０を介して、あるいは入出力Ｉ／Ｆ１４０、ＭＰＥＧコーデック１３０を介して端子６００からトランスポートストリームが入力される。

トランスポートストリームは、ビットストリームパーサー(parser)６０２に入力される。ビットストリームパーサー６０２は、入力トランスポートストリームの中からＰＣＲ(Program Clock Reference)パケットを検出する。ここで、ＰＣＲパケットとは、ＭＰＥＧ２システムズで規定されているＰＣＲが符号化されているパケットである。ＰＣＲパケットは、１００ｍｓｅｃ以内の時間間隔で符号化されている。ＰＣＲは、トランスポートパケットが受信側に到着する時刻を２７ＭＨｚの精度で表す。

そして、２７ＭＨｚＰＬＬ６０３において、記録再生器が持つ２７ＭＨｚクロックをトランスポートストリームのＰＣＲにロック（Lock）させる。タイムスタンプ発生回路６０４は、２７ＭＨｚクロックのクロックのカウント値に基づいたタイムスタンプを発生する。そして、ブロック・シード（Block seed）付加回路６０５は、トランスポートパケットの第１バイト目がスムージングバッファ６０６へ入力される時のタイムスタンプをＡＴＳとして、そのトランスポートパケットに付加する。

ＡＴＳが付加されたトランスポートパケットは、スムージングバッファ６０６を通って、端子６０７から、暗号処理手段１５０に出力され、後段で説明する暗号処理が実行された後、ドライブ１９０（図１）、記録媒体Ｉ／Ｆ２１０（図２）を介してストレージメディアである記録媒体１９５に記録される。

図７は、入力トランスポートストリームが記録媒体に記録される時の処理の例を示す。図７（Ａ）は、ある特定プログラム（コンテンツ）を構成するトランスポートパケットの入力を示す。ここで横軸は、ストリーム上の時刻を示す時間軸である。この例ではトランスポートパケットの入力は、図７（Ａ）に示すように

不規則なタイミングで現れる。

図７（Ｂ）は、ブロック・シード（Block Seed）付加回路６０５の出力を示す。ブロック・シード（Block Seed）付加回路６０５は、トランスポートパケット毎に、そのパケットのストリーム上の時刻を示すＡＴＳを含むブロック・シード（Block Seed）を付加して、ソースパケットを出力する。図７（Ｃ）は記録媒体に記録されたソースパケットを示す。ソースパケットは、図７（Ｃ）に示すように間隔を詰めて記録媒体に記録される。このように間隔を詰めて記録することにより記録媒体の記録領域を有効に使用できる。

図８は、記録媒体１９５に記録されたトランスポートストリームを再生する場合のＴＳ処理手段３００の処理構成ブロック図を示している。端子８００からは、後段で説明する暗号処理手段において復号されたＡＴＳ付きのトランスポートパケットが、ブロック・シード（Block seed）分離回路８０１へ入力され、ＡＴＳとトランスポートパケットが分離される。タイミング発生回路８０４は、再生器が持つ２７ＭＨｚクロック８０５のクロックカウンター値に基づいた時間を計算する。

なお、再生の開始時において、一番最初のＡＴＳが初期値として、タイミング発生回路８０４にセットされる。比較器８０３は、ＡＴＳとタイミング発生回路８０４から入力される現在の時刻を比較する。そして、タイミング発生回路８０４が発生する時間とＡＴＳが等しくなった時、出力制御回路８０２は、そのトランスポートパケットをＭＰＥＧコーデック１３０又はディジタル入出力Ｉ／Ｆ１２０へ出力する。

図９は、入力ＡＶ信号を記録再生器１００のＭＰＥＧコーデック１３０においてＭＰＥＧエンコードして、さらにＴＳ処理手段３００においてトランスポートストリームを符号化する構成を示す。従って図９は、図１又は、図２おけるＭＰＥＧコーデック１３０とＴＳ処理手段３００の両処理構成を併せて示すブロック図である。端子９０１からは、ビデオ信号が入力されており、それはＭＰＥＧビデオエンコーダ９０２へ入力される。

ＭＰＥＧビデオエンコーダ９０２は、入力ビデオ信号をＭＰＥＧビデオストリームに符号化し、それをバッファビデオストリームバッファ９０３へ出力する。

また、ＭＰＥＧビデオエンコーダ９０２は、ＭＰＥＧビデオストリームについてのアクセスユニット情報を多重化スケジューラ９０８へ出力する。ビデオストリームのアクセスユニットとは、ピクチャであり、アクセスユニット情報とは、各ピクチャのピクチャタイプ，符号化ビット量，デコードタイムスタンプである。ここで、ピクチャタイプは、Ｉ／Ｐ／Ｂピクチャ（picture）の情報である。また、デコードタイムスタンプは、ＭＰＥＧ２システムズで規定されている情報である。

端子９０４からは、オーディオ信号が入力されており、それはＭＰＥＧオーディオエンコーダ９０５へ入力される。ＭＰＥＧオーディオエンコーダ９０５は、入力オーディオ信号をＭＰＥＧオーディオストリームに符号化し、それをバッファ９０６へ出力する。また、ＭＰＥＧオーディオエンコーダ９０５は、ＭＰＥＧオーディオストリームについてのアクセスユニット情報を多重化スケジューラ９０８へ出力する。オーディオストリームのアクセスユニットとは、オーディオフレームであり、アクセスユニット情報とは、各オーディオフレームの符号化ビット量，デコードタイムスタンプである。

多重化スケジューラ９０８には、ビデオとオーディオのアクセスユニット情報が入力される。多重化スケジューラ９０８は、アクセスユニット情報に基づいて、ビデオストリームとオーディオストリームをトランスポートパケットに符号化する方法を制御する。多重化スケジューラ９０８は、内部に２７ＭＨｚ精度の基準時刻を発生するクロックを持ち、そして、ＭＰＥＧ２で規定されている仮想的なデコーダモデルであるＴ－ＳＴＤを満たすようにして、トランスポートパケットのパケット符号化制御情報を決定する。パケット符号化制御情報は、パケット化するストリームの種類とストリームの長さである。

パケット符号化制御情報がビデオパケットの場合、スイッチ９７６はａ側になり、ビデオストリームバッファ９０３からパケット符号化制御情報により指示されたペイロードデータ長のビデオデータが読み出され、トランスポートパケット符号化器９０９へ入力される。

パケット符号化制御情報がオーディオパケットの場合、スイッチ９７６はｂ側になり、オーディオストリームバッファ９０６から指示されたペイロードデータ長のオーディオデータが読み出され、トランスポートパケット符号化器９０９へ

入力される。

パケット符号化制御情報がＰＣＲパケットの場合、トランスポートパケット符号化器９０９は、多重化スケジューラ９０８から入力されるＰＣＲを取り込み、ＰＣＲパケットを出力する。パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケット符号化器９０９へは何も入力されない。

トランスポートパケット符号化器９０９は、パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケットを出力しない。それ以外の場合、パケット符号化制御情報に基づいてトランスポートパケットを生成し、出力する。従って、トランスポートパケット符号化器９０９は、間欠的にトランスポートパケットを出力する。到着（Arrival）タイムスタンプ（time stamp）計算手段９１０は、多重化スケジューラ９０８から入力されるＰＣＲに基づいて、トランスポートパケットの第１バイト目が受信側に到着する時刻を示すＡＴＳを計算する。

多重化スケジューラ９０８から入力されるＰＣＲは、ＭＰＥＧ２で規定されるトランスポートパケットの１０バイト目の受信側への到着時刻を示すので、ＡＴＳの値は、ＰＣＲの時刻から１０バイト前のバイトが到着する時刻となる。

ブロック・シード（Block Seed）付加回路９１１は、トランスポートパケット符号化器９０９から出力されるトランスポートパケットにＡＴＳを付加する。ブロック・シード（Block seed）付加回路９１１から出力されるＡＴＳ付きのトランスポートパケットは、スムージングバッファ９１２を通って、暗号処理手段１５０へ入力され、後段で説明する暗号処理が実行された後、ストレージメディアである記録媒体１９５へ格納される。

記録媒体１９５へ格納されるＡＴＳ付きのトランスポートパケットは、暗号処理手段１５０で暗号化される前に図７（Ｃ）に示すように間隔を詰めた状態で入力され、その後、記録媒体１９５に格納される。トランスポートパケットが間隔を詰めて記録されても、ＡＴＳを参照することによって、そのトランスポートパケットの受信側への入力時刻を制御することができる。

ところで、ＡＴＳの大きさは３２ビットに決まっているわけではなく、２４ビ

ット乃至３１ビットでも構わない。ＡＴＳのビット長が長いほど、ＡＴＳの時間カウンターが一周する周期が長くなる。例えば、ＡＴＳが２７ＭＨｚ精度のバイナリーカウンターである場合、２４－ｂｉｔ長のＡＴＳが一周する時間は、約０．６秒である。この時間間隔は、一般のトランスポートストリームでは十分な大きさである。なぜなら、トランスポートストリームのパケット間隔は、ＭＰＥＧ２の規定により、最大０．１秒と決められているからである。しかしながら、十分な余裕を見て、ＡＴＳを２４－ｂｉｔ以上にしてもよい。

このように、ＡＴＳのビット長を様々な長さとした場合、ブロックデータの付加データであるブロックシードの構成としていくつかの構成が可能となる。ブロック・シードの構成例を図１０に示す。図１０の例１は、ＡＴＳを３２ビット分使用する例である。図１０の例２は、ＡＴＳを３０ビットとし、コピー制御情報（CCI）を２ビット分使用する例である。コピー制御情報は、それが付加されたデータのコピー制御の状態を表す情報であり、ＳＣＭＳ：Serial Copy Management SystemやＣＧＭＳ：Copy Generation Management Systemが有名である。これらのコピー制御情報では、その情報が付加されたデータは制限なくコピーが許可されていることを示すコピーフリー（Copy Free）、1世代のみのコピーを許可する1世代コピー許可（One Generation Copy Allowed）、コピーを認めないコピー禁止（Copy Prohibited）などの情報が表せる。

図１０に示す例３は、ＡＴＳを２４ビットとし、ＣＣＩを２ビット使用し、さらに他の情報を６ビット使用する例である。他の情報としては、例えばこのデータがアナログ出力される際に、アナログ映像データのコピー制御機構であるマクロビジョン（Macrovision）のオン／オフ（On/Off）を示す情報など、様々な情報を利用することが可能である。

［記録データの互換性が必要なシステムにおけるデータ記録処理に伴う暗号処理］

次に、記録データの互換性が必要なシステム、即ち、ある記録再生器において記録した記録媒体を他の記録再生器において再生可能とすることが要請されるシステムでのデータ記録処理に伴う暗号処理について説明する。記録データの互換性が必要なシステムは例えば図２に示すような記録再生装置２００であり、記録

媒体１９５が他の記録再生器においても使用可能とする要請があるものである。

このようなシステムにおけるデータ記録処理における暗号化処理について、図１１、図１２の処理ブロック図及び図１３のフローチャートを用いて説明する。ここでは、記録媒体として光ディスクを例とする。この実施例は、特開平１１－２２４４６１号公報（特願平１０－２５３１０号）に記載した構成と同様に、ある記録再生装置で記録したデータを、別の記録再生装置で再生できることが必要な、即ち記録データの互換性が必要なシステムである。そして、記録媒体上のデータのbit-by-bitコピーを防ぐために、記録媒体固有の識別情報としてのディスクＩＤ(Disc ID)を、データを暗号化する鍵に作用させるようにしている。

図１１、図１２の処理ブロック図に従って、暗号処理手段１５０が実行するデータの暗号化処理の概要について説明する。

記録再生装置１１００は自身のメモリ１８０（図２参照）に格納しているマスターキー１１０１を読み出す。マスターキー１１０１は、ライセンスを受けた記録再生装置に格納された秘密キーであり、複数の記録再生装置に共通なキー、即ちシステム全体で共通なキーである。記録再生装置１１００は例えば光ディスクである記録媒体１１２０に識別情報としてのディスクＩＤ（Disc ID）１１０３が既に記録されているかどうかを検査する。記録されていれば、ディスクＩＤ（Disc ID）１１０３を読み出し（図１１に相当）、記録されていなければ、暗号処理手段１５０においてランダムに、もしくは予め定められた例えば乱数発生等の方法でディスクＩＤ（Disc ID）１２０１を生成し、ディスクに記録する（図１２に相当）。ディスクＩＤ（Disc ID）１１０３はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。

記録再生器１１００は、次にマスターキーとディスクＩＤを用いて、ディスク固有キー（Disc Unique Key）を生成１１０２する。ディスク固有キー（Disc Unique Key）の具体的な生成方法としては、例えば、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクＩＤ（Disc ID）とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみをディスク固有キー（Disc Unique Key）として使用する方法や、ブロック暗号関数を用いたハッシュ関数にマスターキー（Master Key）とディスクＩＤ（Di

sc ID）を入力して得られた結果を用いるなどの方法が挙げられる。

次に、記録毎の固有鍵であるタイトルキー（Title Key）を暗号処理手段１５０においてランダムに、もしくは予め定められた例えば乱数発生等の方法で生成１１０４し、ディスク１１２０に記録する。ディスク上には、どこのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキーを格納することができる。

次にディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）から、タイトル固有キー（Title Unique Key）を生成する。この生成の具体的な方法も、上記のように、SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法など、幾つ挙げることができる。

なお、上記の説明では、マスターキー（Master Key）とディスクＩＤ（Disc ID）からディスク固有キー（Disc Unique Key）を生成し、これとタイトルキー（Title Key）からタイトル固有キー（Title Unique Key）をそれぞれ生成するようにしているが、ディスク固有キー（Disc Unique Key）を不要としてマスターキー（Master Key）とディスクＩＤ（Disc ID）とタイトルキー（Title Key）から直接タイトル固有キー（Title Unique Key）を生成してもよく、また、タイトルキー（Title Key）を用いずに、マスターキー（Master Key）とディスクＩＤ（Disc ID）からタイトル固有キー（Title Unique Key）相当の鍵を生成してもよい。

ところで、例えば上記の５ＣＤＴＣＰに規定される伝送フォーマットのひとつを使用した場合、データはＭＰＥＧ２のＴＳパケットで伝送される場合がある。例えば、衛星放送を受信したセットトップボックス（ＳＴＢ：Set Top Box）がこの放送を記録機に５ＣＤＴＣＰを用いて伝送する際に、ＳＴＢは衛星放送通信路で伝送されたＭＰＥＧ２　ＴＳパケットをIEEE1394上も伝送することが、データ変換の必要がなく望ましい。

記録再生装置１１００は記録すべきコンテンツデータをこのＴＳパケットの形で受信し、前述したＴＳ処理手段３００において、各ＴＳパケットを受信した時刻情報であるＡＴＳを付加する。なお、先に説明したように、ブロックデータに付加されるブロック・シードは、ＡＴＳとコピー制御情報、さらに他の情報を組み合わせた値から構成してもよい。

ＡＴＳを付加したＴＳパケットをＸ個（例えばＸ＝３２）並べて、１ブロックのブロックデータが形成（図５の上の図参照）され、図１１、１２の下段に示すように、被暗号化データとして入力されるブロックデータの先頭の第１～４バイトが分離され（セレクタ１１０８）て出力される３２ビットのＡＴＳを含むブロックシード（Block Seed）と、先に生成したタイトル固有キー（Title Unique Key）とから、そのブロックのデータを暗号化する鍵であるブロック・キー（Block Key）が生成１１０７される。

ブロック・キー（Block Key）の生成方法の例を図１４に示す。図１４では、いずれも３２ビットのブロック・シード（Block Seed）と、６４ビットのタイトル固有キー（Title Unique Key）とから、６４ビットのブロックキー（Block Key）を生成する例を２つ示している。

上段に示す例１は、鍵長６４ビット、入出力がそれぞれ６４ビットの暗号関数を使用している。タイトル固有キー（Title Unique Key）をこの暗号関数の鍵とし、ブロックシード（Block Seed）と３２ビットの定数（コンスタント）を連結した値を入力して暗号化した結果をブロックキー（Block Key）としている。

例２は、FIPS 180-1のハッシュ関数SHA-1を用いた例である。タイトル固有キー（Title Unique Key）とブロックシード（Block Seed）を連結した値をSHA-1に入力し、その１６０ビットの出力を、例えば下位６４ビットのみ使用するなど、６４ビットに縮約したものをブロックキー（Block Key）としている。

なお、上記ではディスク固有キー（Disc Unique key）、タイトル固有キー（Title Unique Key）、ブロックキー（Block Key）をそれぞれ生成する例を説明したが、例えば、ディスク固有キー（Disc Unique Key）とタイトル固有キー（Title Unique Key）の生成を実行することなく、ブロック毎にマスターキー（Master Key）とディスクＩＤ（Disc ID）とタイトルキー（Title Key）とブロックシード（Block Seed）を用いてブロックキー（Block Key）を生成してもよい。

ブロックキーが生成されると、生成されたブロックキー（Block Key）を用いてブロックデータを暗号化する。図１１、１２の下段に示すように、ブロックシード（Block Seed）を含むブロックデータの先頭の第１～ｍバイト（例えばｍ＝８バイト）は分離（セレクタ１１０８）されて暗号化対象とせず、ｍ＋１バイト目

から最終データまでを暗号化１１０９する。なお、暗号化されないｍバイト中にはブロック・シードとしての第１～４バイトも含まれる。セレクタ１１０８により分離された第ｍ＋１バイト以降のブロックデータは、暗号処理手段１５０に予め設定された暗号化アルゴリズムに従って暗号化１１０９される。暗号化アルゴリズムとしては、例えばFIPS 46-2で規定されるＤＥＳ（Data Encryption Standard）を用いることができる。

ここで、使用する暗号アルゴリズムのブロック長（入出力データサイズ）がＤＥＳのように８バイトであるときは、Ｘを例えば３２とし、ｍを例えば８の倍数とすることで、端数なくｍ＋１バイト目以降のブロックデータ全体が暗号化できる。

即ち、１ブロックに格納するＴＳパケットの個数をＸ個とし、暗号アルゴリズムの入出力データサイズをＬバイトとし、ｎを任意の自然数とした場合、１９２＊Ｘ＝ｍ＋ｎ＊Ｌが成り立つようにＸ，ｍ、Ｌを定めることにより、端数処理が不要となる。

暗号化した第ｍ＋１バイト以降のブロックデータは暗号処理のされていない第１～ｍバイトデータとともにセレクタ１１１０により結合されて暗号化コンテンツ１１１２として記録媒体１１２０に格納される。

以上の処理により、コンテンツはブロック単位でＡＴＳを含むブロック・シードに基づいて生成されるブロック鍵で暗号化が施されて記録媒体に格納されることになる。先にも説明したようにＡＴＳはブロック固有のランダム性の高いデータであるので、各ブロックに設定されたＡＴＳに基づくブロック鍵は、それぞれが異なった鍵となる。即ち、ブロック毎に暗号鍵が変更され、このため暗号解析に対する強度を高めることができる。また、ブロック・シードを暗号鍵生成データとして使用することにより、ブロック毎の暗号鍵をデータと別に保存しておく必要がなく、そのため暗号鍵の保存領域が不要となり記憶領域を節約できる。また、ブロック・シードはコンテンツデータとともに書き込み読み出しが実行されるデータであるので、従来のように暗号鍵を別領域に保存する構成とは異なり、記録再生時に暗号鍵データを書き込んだり読み出したりする処理が省略でき効率的な処理が可能となる。

次に図１３に示すフローチャートに従って、データ記録処理に伴って実行されるＴＳ処理手段３００におけるＡＴＳ付加処理及び暗号処理手段１５０における暗号処理の処理の流れを説明する。図１３のＳ１３０１において、記録再生装置は自身のメモリ１８０に格納しているマスターキーを読み出す。

Ｓ１３０２において、記録媒体に識別情報としてのディスクＩＤ（Disc ID）が既に記録されているかどうかを検査する。記録されていればＳ１３０３でこのディスクＩＤを読み出し、記録されていなければＳ１３０４で、ランダムに、もしくは予め定められた方法でディスクＩＤを生成し、ディスクに記録する。次に、Ｓ１３０５では、マスターキーとディスクＩＤを用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1で定められているハッシュ関数SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法などを適用することで求める。

次にＳ１３０６に進み、その一回の記録毎の固有の鍵としてタイトルキー（Title Key）を生成しディスクに記録する。次にＳ１３０７で、上記のディスク固有キーとタイトルキーから、タイトル固有キーを生成する。キー生成には、SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法を適用する。

Ｓ１３０８では、記録再生装置は記録すべきコンテンツデータの被暗号化データをＴＳパケットの形で受信する。Ｓ１３０９で、ＴＳ処理手段３００は、各ＴＳパケットを受信した時刻情報であるＡＴＳを付加する。あるいはコピー制御情報ＣＣＩとＡＴＳ、さらに他の情報を組み合わせた値を付加する。次に、Ｓ１３１０で、ＡＴＳを付加したＴＳパケットを順次受信し、１ブロックを形成する例えばＸ＝３２に達したか、あるいはパケットの終了を示す識別データを受信したかを判定する。いずれかの条件が満足された場合はステップＳ１３１１に進み、Ｘ個、あるいはパケット終了までのパケットを並べて、１ブロックのブロックデータを形成する。

次に、暗号処理手段１５０は、Ｓ１３１２で、ブロックデータの先頭の３２ビット（ＡＴＳを含むブロック・シード）とＳ１３０７で生成したタイトル固有キーとから、そのブロックのデータを暗号化する鍵であるブロックキーを生成する。

Ｓ１３１３では、ブロックキーを用いてＳ１３１１で形成したブロックデータ

を暗号化する。なお、先にも説明したように、暗号化の対象となるのは、ブロックデータのｍ＋１バイト目から最終データまでである。暗号化アルゴリズムは、例えばFIPS 46-2で規定されるＤＥＳ（Data Encryption Standard）が適用される。

Ｓ１３１４で、暗号化したブロックデータを記録媒体に記録する。Ｓ１３１５で、全データを記録したかを判断する。全データを記録していれば、記録処理を終了し、全データを記録していなければＳ１３０８に戻って残りのデータの処理を実行する。

［記録データの互換性が必要なシステムにおけるデータ再生処理に伴う暗号処理］

次に、上記のようにして記録媒体に記録された暗号化コンテンツを復号して再生する処理について図１５の処理ブロック図と、図１６のフローチャートを用いて説明する。

まず、図１５に示す処理ブロック図に従って説明する。記録再生装置１５００はディスク１５２０からディスクＩＤ１５０２を、また自身のメモリからマスターキー１５０１を読み出す。先の記録処理の説明から明らかなように、ディスクＩＤはディスクに記録されているか、記録されていない場合は記録再生器において生成してディスクに記録したディスク固有の識別子である。マスターキー１５０１は、ライセンスを受けた記録再生装置に格納された秘密キーである。

記録再生装置１５００は、次に、ディスクＩＤ（Disc ID）とマスターキー（Master Key）を用いてディスク固有キー（Disc Unique Key）を生成１５０３する。このキー生成方法は、例えば、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクＩＤ（Disc ID）とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみをディスク固有キー（Disc Unique Key）として使用する方法や、ブロック暗号関数を用いたハッシュ関数にマスターキー（Master Key）とディスクＩＤ（Disc ID）を入力して得られた結果を用いるなどの方法が挙げられる。

次に、ディスクから読み出すべきデータに対応して記録されたタイトルキー（Title Key）１５０４を読み出し、タイトルキー（Title Key）１５０４とディスク固有キー（Disc Unique Key）からタイトル固有キー（Title Unique Key）を

生成１５０５する。この生成方法も、ハッシュ関数SHA-1、ブロック暗号関数を用いたハッシュ関数の適用が可能である。

なお、上記の説明では、マスターキー（Master Key）とディスクＩＤ（Disc ID）からディスク固有キー（Disc Unique Key）を生成し、これとタイトルキー（Title Key）からタイトル固有キー（Title Unique Key）をそれぞれ生成するようにしているが、ディスク固有キー（Disc Unique Key）を不要としてマスターキー（Master Key）とディスクＩＤ（Disc ID）とタイトルキー（Title Key）から直接タイトル固有キー（Title Unique Key）を生成してもよく、また、タイトルキー（Title Key）を用いずに、マスターキー（Master Key）とディスクＩＤ（Disc ID）からタイトル固有キー（Title Unique Key）相当の鍵を生成してもよい。

次にディスクに格納されている暗号化コンテンツ１５０７から順次ブロックデータ（Block Data）を読み出し、ブロックデータ（Block Data）の先頭の４バイトを構成するブロック・シード（Block Seed）をセレクタ１５０８において分離して、タイトル固有キー（Title Unique Key）との相互処理により、ブロックキー（Block Key）を生成する。

ブロック・キー（Block Key）の生成方法は、先に説明した図１４の構成を適用することができる。即ち、３２ビットのブロック・シード（Block Seed）と、６４ビットのタイトル固有キー（Title Unique Key）とから、６４ビットのブロックキー（Block Key）を生成する構成が適用できる。

なお、上記ではディスク固有キー（Disc Unique key）、タイトル固有キー（Title Unique Key）、ブロックキー（Block Key）をそれぞれ生成する例を説明したが、例えば、ディスク固有キー（Disc Unique Key）とタイトル固有キー（Title Unique Key）の生成を実行することなく、ブロック毎にマスターキー（Master Key）とディスクＩＤ（Disc ID）とタイトルキー（Title Key）とブロックシード（Block Seed）を用いてブロックキー（Block Key）を生成してもよい。

ブロックキーが生成されると、ブロックキー（Block Key）を用いて暗号化されているブロックデータを復号１５０９し、セレクタ１５１０を介して復号データとして出力する。なお、復号データには、トランスポートストリームを構成する各トランスポートパケットにＡＴＳが付加されており、先に説明したＴＳ処理手

段３００において、ＡＴＳに基づくストリーム処理が実行される。その後、データは、使用、例えば、画像を表示したり、音楽を鳴らしたりすることが可能となる。

このように、ブロック単位で暗号化され記録媒体に格納された暗号化コンテンツはブロック単位でＡＴＳを含むブロック・シードに基づいて生成されるブロック鍵で復号処理が施されて再生が可能となる。

次に図１６に示すフローチャートに従って、復号処理及び再生処理について、処理の流れを説明する。図１６のＳ１６０１において、記録再生装置はディスクからディスクＩＤを、また自身のメモリからマスターキーを読み出す。Ｓ１６０２で、ディスクＩＤとマスターキーを用いてディスク固有キーを生成する。

次にＳ１６０３で、ディスクから読み出すべきデータのタイトルキーを読み出し、Ｓ１６０４で、タイトルキーとディスク固有キーからタイトル固有キーを生成する。次にＳ１６０５でディスクから暗号化されて格納されているブロックデータを読み出す。Ｓ１６０６で、ブロックデータの先頭の４バイトのブロックシード（Block Seed）と、Ｓ１６０４で生成したタイトル固有キーを用いてブロックキーを生成する。

次に、Ｓ１６０７で、ブロックキーを用いて暗号化されているブロックデータを復号し、Ｓ１６０８で、全データを読み出したかを判断し、全データを読み出していれば終了し、そうでなければＳ１６０５に戻り残りのデータを読み出す。

［記録されたデータの互換性が必要ないシステムにおけるデータ記録処理に伴う暗号処理］

次に、記録データの互換性が必要ないシステム、即ち、ある記録再生器において記録した記録媒体を他の記録再生器において再生可能とすることが要請されないシステム、即ち、記録データはそれを記録した装置でのみ読み出しができればよいシステムでのデータ記録処理に伴う暗号処理について図１７の処理ブロック図及び図１８のフローチャートを用いて説明する。

図１７の処理ブロック図を参照しながら、図１８のフローチャートの処理手順に従って順次説明する。

まず、図１８のＳ１８０１において、記録再生装置１７００（図１７参照）は、

その装置固有の鍵であるデバイス固有キー（Device Unique Key）を生成する。

図１７に示すようにデバイス固有キー（Device Unique Key）の生成はＬＳＩキー、デバイスキー、メディアキー、ドライブキーのいずれか、又はこれらの任意の組合わせデータに基づいて生成する。ＬＳＩキーは、暗号処理手段１５０（図１参照）を構成するＬＳＩに対してＬＳＩの製造時に格納されたキーである。デバイス・キーは記録再生器の製造時にフラッシュメモリ、ＥＥＰＲＯＭ等の記憶素子に格納されたデバイス即ち記録再生器に対応して設定されたキーである。メディアキーはコンテンツを格納する記録媒体に対して設定され記録媒体に格納されたキーである。ドライブキーは、ＤＶＤドライブ等、記録媒体のドライブ装置に対して付与されたキーである。

本実施例では、デバイス固有キー（Device Unique Key）を、ＬＳＩキー、デバイスキー、メディアキー、ドライブキーのいずれか、又はこれらの任意の組合わせデータに基づいて生成する。

例えば、ＬＳＩキーとデバイスキーを使用したデバイス固有キーの生成処理について図１９を用いて説明する。図１９は、例えば図１の暗号処理手段Ｉ５０をＬＳＩとして構成した暗号処理手段ＬＳＩ１９００における処理例を示している。

ＬＳＩキー記憶部１９０１は、複数の暗号処理手段ＬＳＩに共通（従って、複数の記録再生装置にも共通）のＬＳＩキーを記憶している。具体的には例えば、ＬＳＩ製造時のロット毎に一律のキーが格納される。また、すべての暗号処理手段Ｌ.ＳＩに共通のＬＳＩキーを記憶する構成としてもよいし、幾つかの暗号処理手段ＬＳＩのグループ毎に共通のＬＳＩキーを記憶するようにしてもよい。ＬＳＩキーを、幾つの暗号処理手段ＬＳＩに共通とするかは、例えば、暗号処理手段ＬＳＩの製造コストとの関係で決めることができる。

暗号処理手段ＬＳＩ１９００の鍵生成部は、キー記憶部１９０１に記憶されているＬＳＩキーを読み出すとともに、暗号処理手段ＬＳＩ１９００の外部の記憶素子としての例えば記録再生装置のＲＯＭに記憶されているデバイスキー１９１０を、バスを介して読み出すことで取得し、このＬＳＩキー及びデバイスキーに対して、キーを生成するための関数（鍵生成関数）を適用して、デバイス固有キー（Device Unique Key）を生成する。

なお、鍵生成関数としては、ＬＳＩキー及びデバイスキーから、デバイス固有キー（Device Unique Key）を計算することは容易であるが、その逆に、デバイス固有キー（Device Unique Key）から、ＬＳＩキーやデバイスキーを計算することはできない一方向性関数を用いることができる。具体的には、デバイス固有キー生成部１９０２は、例えば、FIPS180-1のSHA-1ハッシュ関数等の一方向性関数に対して、ＬＳＩキーとデバイスキーとを連結したものを入力として与えて、そのハッシュ関数を演算することにより、デバイス固有キー（Device Unique Key）を生成する。デバイス固有キー（Device Unique Key）は、例えば、FIPS46-2，FIPS46-3のDES，Triple-DES等を利用した一方向性関数を用い、ＬＳＩキーで、デバイスキーを暗号化することにより求めてもよい。

このようにして得られたデバイス固有キー（Device Unique Key）と、コンテンツデータの付加データとして設定されたブロック・シードとによりブロックキーを生成して、生成したブロックキーに基づいて暗号化処理又は復号処理を実行して暗号化コンテンツ１９０６の記録媒体１９２０に対する格納処理、あるいは暗号化コンテンツ１９０６の記録媒体１９２０からの再生処理を実行する。

コンテンツを暗号化方式、及び復号方式としては、例えば、FIPS46-2に挙げられているデータ・エンクリプション・スタンダード(Data Encryption Standard)その他を用いることが可能である。

図１９は、ＬＳＩキー及びデバイスキーから、デバイス固有キー（Device Unique Key）を生成する例であるが、例えば、記録媒体に固有の値としてのメディアキーが割り当てられている場合や、記録媒体のドライブに対する固有の値としてのドライブキーが割り当てられている場合には、デバイス固有キー（Device Unique Key）の生成に、そのメディアキーやドライブキーも用いることが可能である。

デバイス固有キー（Device Unique Key）を、ＬＳＩキー及びデバイスキーの他に、メディアキー及びドライブキーのすべてを用いて生成する場合の処理構成例を図２０に示す。図２０は、ISO/IEC9797で規定されているデータインテグリティメカニズム(ＤＩＭ：Data Ingegrity Mechanism)によって、デバイス固有キー（Device Unique Key）を生成する処理構成例を示している。

暗号化部２００１は、ＬＳＩキーを、デバイスキーで暗号化し、演算器２００

４に出力する。演算器２００４は、暗号化部２００１の出力と、メディアキーとを排他的論理和し、暗号化部２００２に供給する。暗号化部２００２は、ＬＳＩキーを鍵とし、演算器２００４の出力を暗号化し、演算器２００５に出力する。演算器２００５は、暗号化部２００２の出力と、ドライブキーとを排他的論理和し、暗号化部２００３に出力する。暗号化部２００３は、ＬＳＩキーを鍵とし、演算器２００５の出力を暗号化し、その暗号化結果を、デバイス固有キー（Device Unique Key）として出力する。

図１８に戻り、データ記録処理ステップの説明を続ける。ステップＳ１８０１では、上述のようにＬＳＩキー、デバイスキー、メディアキー、ドライブキーのいずれか、又はこれらの任意の組合わせデータに基づいてデバイス固有キーを生成する。

Ｓ１８０２では、記録再生装置は記録すべきコンテンツデータの被暗号化データをＴＳパケットの形で受信する。Ｓ１８０３で、ＴＳ処理手段３００は、各ＴＳパケットを受信した時刻情報であるＡＴＳを付加する。あるいはコピー制御情報ＣＣＩとＡＴＳ、さらに他の情報を組み合わせた値を付加する。次に、Ｓ１８０４で、ＡＴＳを付加したＴＳパケットを順次受信し、１ブロックを形成する例えばＸ＝３２に達したか、あるいはパケットの終了を示す識別データを受信したかを判定する。いずれかの条件が満足された場合はステップＳ１８０５に進み、Ｘ個、あるいはパケット終了までのパケットを並べて、１ブロックのブロックデータを形成する。

次に、Ｓ１８０６で、暗号処理手段１５０は、ブロックデータの先頭の３２ビット（ＡＴＳを含むブロック・シード）とＳ１８０１で生成したデバイス固有キーとから、そのブロックのデータを暗号化する鍵であるブロックキーを生成する。

Ｓ１８０７では、ブロックキーを用いてＳ１８０５で形成したブロックデータを暗号化する。なお、先にも説明したように、暗号化の対象となるのは、ブロックデータのｍ＋１バイト目から最終データまでである。暗号化アルゴリズムは、例えばFIPS 46-2で規定されるＤＥＳ（Data Encryption Standard）が適用される。

Ｓ１８０８で、暗号化したブロックデータを記録媒体に記録する。Ｓ１８０９で、全データを記録したかを判断する。全データを記録していれば、記録処理を

終了し、全データを記録していなければＳ１８０２に戻って残りのデータの処理を実行する。

［記録されたデータの互換性が必要ないシステムにおけるデータ再生処理に伴う暗号処理］

次に、このようにして記録されたデータの再生処理について、図２１の処理ブロック図及び図２２のフローチャートを用いて説明する。

図２１の処理ブロック図を参照しながら、図２２のフローチャートの処理手順に従って順次説明する。

まず、図２２のＳ２２０１において、記録再生装置２１００（図２１参照）は、その装置固有の鍵であるデバイス固有キー（Device Unique Key）を生成する。

図２１に示すようにデバイス固有キー（Device Unique Key）の生成はＬＳＩキー、デバイスキー、メディアキー、ドライブキーのいずれか、又はこれらの任意の組合わせデータに基づいて生成２１０１する。ここで各キーは先に説明した通り、ＬＳＩキーは、暗号処理手段１５０（図１、図２参照）を構成するＬＳＩに対してＬＳＩの製造時に格納されたキー、デバイス・キーは記録再生器の製造時にフラッシュメモリ、ＥＥＰＲＯＭ等の記憶素子に格納されたデバイスに対応して設定されたキー、メディアキーはコンテンツを格納する記録媒体に対して設定され記録媒体に格納されたキー、ドライブキーは、ＤＶＤドライブ等、記録媒体のドライブ装置に対して付与されたキーである。

次にＳ２２０２でディスクから暗号化されて格納されているブロックデータを読み出す。Ｓ２２０３で、ブロックデータの先頭の４バイトのブロックシード（Block Seed）と、Ｓ２２０１で生成したデバイス固有キーを用いてブロックキーを生成（図２１の２１０２）する。

次に、Ｓ２２０４で、ブロックキーを用いて暗号化されているブロックデータを復号（図２１の２１０５）し、Ｓ２２０５で、全データを読み出したかを判断し、全データを読み出していれば終了し、そうでなければＳ２２０２に戻り残りのデータを読み出す。

なお、この処理においても記録媒体２１２０に格納された暗号化コンテンツ２１０３はブロックデータの先頭第１～４バイトのブロックシードがセレクタ２１

０４において分離され、また暗号化されていない第１～ｍバイトデータは、復号処理を実行されずに、セレクタ２１０６において結合されて出力される。復号データには、パケット毎に入力タイミングを表すＡＴＳ（Arrival Time Stamp：着信時刻スタンプ）が付加されており、前述のＴＳ処理手段における処理により正常な再生が可能となる。

このように、本発明の構成では、ブロックデータの先頭のＴＳパケットの受信時刻によって変化するＡＴＳに基づいて変化するブロックキーによって、コンテンツを暗号化するようにしたので、仮に、あるコンテンツの暗号化に用いたブロックキーが漏洩しても、他のコンテンツの保護に影響はない。従来のシステムのようにひとつの暗号鍵をすべてのコンテンツの暗号化に使用した場合、コンテンツが、常に、固定のデータキーによって暗号化されるため、例えば、ある平文のコンテンツと、それを、データキーによって暗号化した暗号文のコンテンツとの組が、違法コピーを行おうとする者に入手された場合に、いわゆる線形攻撃や差分攻撃といった暗号攻撃法を用いて、データキーが解読され、これにより、そのデータキーによって暗号化した暗号化コンテンツすべてが復号され、違法にコピーされるおそれがあるが、本発明の構成では、各ブロック単位で暗号鍵が異なるため、このような自体の発生する可能性はほとんどない。

本発明の構成では、ひとつの暗号鍵で暗号化されるデータの量が１ブロックであり、極めて少ないデータ量であるため、いわゆる線形攻撃や差分攻撃といった暗号攻撃法を用いて鍵を求めることが非常に困難になる。

さらに、本発明の構成では、本来のデータの付加情報として設定されるＡＴＳに基づいて暗号鍵を生成しているので、ブロック毎に暗号鍵を変化させる構成としても、その暗号鍵を記録媒体のデータセクタのセクタヘッダ部などに新たに記録する必要がないため、余分な記録容量を消費せず、また記録、再生時にブロック毎の暗号鍵のリード、ライトなどの処理を行う必要がない。

［記録されたデータ再生についての機器制限の設定が可能なシステムにおけるデータ暗号化及び記録処理］

上述の構成は、マスターキーによりブロックキーを生成可能とした構成であり、共通のマスターキーを有する記録再生器においては、再生が可能となる。しかし、

ある特定のデータについては、データ記録を実行したその記録再生器でのみ再生可能としたい場合がある。以下では、このような機器制限の設定を実行する構成について説明する。

本例は、例えば先に説明した図１、図２の記録再生器において記録媒体１９５が着脱可能であり、記録媒体１９５を他の記録再生器にも装着可能な構成において効果的なシステムである。即ち、記録媒体１９５に対してデータを記録したとき、その記録データを記録した記録媒体を他の記録再生器に装着した場合に再生可能とするか再生不可能とするかを設定可能としたものである。

このようなシステムにおけるデータ記録処理における暗号化処理について、図２３、図２４の処理ブロック図及び図２５のフローチャートを用いて説明する。ここでは、記録媒体として光ディスクを例とする。この実施例では、記録媒体上のデータのbit-by-bitコピーを防ぐために、記録媒体固有の識別情報としてのディスクＩＤ(Disc ID)を、データを暗号化する鍵に作用させるようにしている。

図２３、図２４の処理ブロック図に従って、暗号処理手段１５０が実行するデータの暗号化処理の概要について説明する。

記録再生装置２３００は自身のメモリ１８０（図１，２参照）に格納しているマスターキー２３０１、デバイス識別子としてのデバイスＩＤ２３３１、デバイス固有キー２３３２を読み出す。マスターキー２３０１は、ライセンスを受けた記録再生装置に格納された秘密キーであり、複数の記録再生装置に共通なキー、即ちシステム全体で共通なキーである。デバイスＩＤは記録再生装置２３００の識別子であり、予め記録再生装置に格納されている例えば製造番号等の識別子である。このデバイスＩＤは公開されていてもよい。デバイス固有キーは、その記録再生器２３００に固有の秘密鍵であり、予め個々の記録再生装置に応じて異なるように設定されて格納されたキーである。これらは予め記録再生装置２３００のメモリに格納されている。

記録再生装置２３００は例えば光ディスクである記録媒体２３２０に識別情報としてのディスクＩＤ（Disc ID）２３０３が既に記録されているかどうかを検査する。記録されていれば、ディスクＩＤ（Disc ID）２３０３を読み出し（図２３に相当）、記録されていなければ、暗号処理手段１５０においてランダムに、も

しくは予め定められた例えば乱数発生等の方法でディスクＩＤ（Disc ID）２４０１を生成し、ディスクに記録する（図２４に相当）。ディスクＩＤ（Disc ID）２３０３はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。

記録再生器２３００は、次にマスターキーとディスクＩＤを用いて、ディスク固有キー（Disc Unique Key）を生成２３０２する。ディスク固有キー（Disc Unique Key）の具体的な生成方法としては、図２６に示すように、ブロック暗号関数を用いたハッシュ関数にマスターキー（Master Key）とディスクＩＤ（Disc ID）を入力して得られた結果を用いる例１の方法や、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクＩＤ（Disc ID）とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみをディスク固有キー（Disc Unique Key）として使用する例２の方法が適用できる。

次に、記録毎の固有鍵であるタイトルキー（Title Key）を暗号処理手段１５０においてランダムに、もしくは予め定められた例えば乱数発生等の方法で生成２３０４し、ディスク２３２０に記録する。

さらに、このタイトル（データ）がデータ記録を実行した記録再生装置でのみ再生可能とする（機器制限あり）か、他の機器においても再生可能とする（再生機器制限なし）のいずれであるかを示すフラグ、即ち再生機器制限フラグ（Player Restriction Flag）を設定し２３３３、ディスク2.３２０に記録する２３３５。さらに、機器識別情報としてのデバイスＩＤを取り出して２３３１、ディスク２３２０に記録する２３３４。

ディスク上には、どこのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキー２３０５、再生機器制限フラグ２３３５、デバイスＩＤ２３３４を格納することができる。

次にディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイスＩＤ、あるいは、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイス固有キー、いずれかの組合せから、タイトル固有キー（Title Unique Key）を生成する。

即ち、再生機器制限をしない場合には、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイスＩＤとからタイトル固有キー（Title Unique Key）を生成し、再生機器制限をする場合には、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイス固有キーとからタイトル固有キー（Title Unique Key）を生成する。

このタイトル固有キー（Title Unique Key）生成の具体的な方法は、図２８に示すように、ブロック暗号関数を用いたハッシュ関数にタイトルキー（Title Key）とディスク固有キー（Disc Unique Key）と、デバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）を入力して得られた結果を用いる例１の方法や、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクＩＤ（Disc ID）とデバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみをタイトル固有キー（Title Unique Key）として使用する例２の方法が適用できる。

なお、上記の説明では、マスターキー（Master Key）とディスクＩＤ（Disc ID）からディスク固有キー（Disc Unique Key）を生成し、これとタイトルキー（Title Key）とデバイスＩＤ、もしくはタイトルキー（Title Key）とデバイス固有キーからタイトル固有キー（Title Unique Key）をそれぞれ生成するようにしているが、ディスク固有キー（Disc Unique Key）を不要としてマスターキー（Master Key）とディスクＩＤ（Disc ID）とタイトルキー（Title Key）と、デバイスＩＤもしくはデバイス固有キーから直接タイトル固有キー（Title Unique Key）を生成してもよく、また、タイトルキー（Title Key）を用いずに、マスターキー（Master Key）とディスクＩＤ（Disc ID）と、デバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）からタイトル固有キー（Title Unique Key）相当の鍵を生成してもよい。

例えば上記の５ＣＤＴＣＰに規定される伝送フォーマットのひとつを使用した場合、データはＭＰＥＧ２のＴＳパケットで伝送される場合がある。例えば、衛星放送を受信したセットトップボックス（ＳＴＢ：Set Top Box）がこの放送を記

録機に５ＣＤＴＣＰを用いて伝送する際に、ＳＴＢは衛星放送通信路で伝送されたＭＰＥＧ２　ＴＳパケットをIEEE1394上も伝送することが、データ変換の必要がなく望ましい。

記録再生装置２３００は記録すべきコンテンツデータをこのＴＳパケットの形で受信し、前述したＴＳ処理手段３００において、各ＴＳパケットを受信した時刻情報であるＡＴＳを付加する。なお、先に説明したように、ブロックデータに対する付加情報としてのブロック・シードとしてＡＴＳとコピー制御情報、さらに他の情報を組み合わせた値を付加する構成としてもよい。

ＡＴＳを付加したＴＳパケットをＸ個（例えばＸ＝３２）並べて、１ブロックのブロックデータが形成（図５の上の図参照）され、図２３、２４の下段に示すように、被暗号化データとして入力されるブロックデータの先頭の第１～４バイトが分離され（セレクタ１１０８）て出力される３２ビットのＡＴＳを含むブロックシード（Block Seed）と、先に生成したタイトル固有キー（Title Unique Key）とから、そのブロックのデータを暗号化する鍵であるブロック・キー（Block Key）が生成２３０７される。ブロック・キー（Block Key）の生成方法は先に説明した図１４の方法が適用可能である。

なお、上記ではディスク固有キー（Disc Unique key）、タイトル固有キー（Title Unique Key）、ブロックキー（Block Key）をそれぞれ生成する例を説明したが、例えば、ディスク固有キー（Disc Unique Key）とタイトル固有キー（Title Unique Key）の生成を実行することなく、ブロック毎にマスターキー（Master Key）とディスクＩＤ（Disc ID）とタイトルキー（Title Key）とブロックシード（Block Seed）と、デバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）を用いてブロックキー（Block Key）を生成してもよい。

ブロックキーが生成されると、生成されたブロックキー（Block Key）を用いてブロックデータを暗号化する。図２３、２４の下段に示すように、ブロックシード（Block Seed）を含むブロックデータの先頭の第１～ｍバイト（例えばｍ＝８バイト）は分離（セレクタ２３０８）されて暗号化対象とせず、ｍ＋１バイト目から最終データまでを暗号化２３０９する。なお、暗号化されないｍバイト中に

はブロック・シードとしての第１～４バイトも含まれる。セレクタ２３０８により分離された第ｍ＋１バイト以降のブロックデータは、暗号処理手段１５０に予め設定された暗号化アルゴリズムに従って暗号化２３０９される。暗号化アルゴリズムとしては、例えばFIPS 46-2で規定されるＤＥＳ（Data Encryption Standard）を用いることができる。

ここで、使用する暗号アルゴリズムのブロック長（入出力データサイズ）がＤＥＳのように８バイトであるときは、Ｘを例えば３２とし、ｍを例えば８の倍数とすることで、端数なくｍ＋１バイト目以降のブロックデータ全体が暗号化できる。

即ち、１ブロックに格納するＴＳパケットの個数をＸ個とし、暗号アルゴリズムの入出力データサイズをＬバイトとし、ｎを任意の自然数とした場合、１９２＊Ｘ＝ｍ＋ｎ＊Ｌが成り立つようにＸ，ｍ、Ｌを定めることにより、端数処理が不要となる。

暗号化した第ｍ＋１バイト以降のブロックデータは暗号処理のされていない第１～ｍバイトデータとともにセレクタ２３１０により結合されて暗号化コンテンツ２３１２として記録媒体１１２０に格納される。

以上の処理により、コンテンツはブロック単位でＡＴＳを含むブロック・シードに基づいて生成されるブロック鍵で暗号化が施されて記録媒体に格納される。また、ブロック鍵は、再生機器制限をしない場合は、デバイスＩＤに基づいて生成され、再生機器制限をする場合は、デバイス固有キーに基づいて生成される。これらの暗号化データは、再生機器制限をした場合は、そのデータを記録した機器でのみ再生可能となる。

即ち、再生機器制限なしの場合は、ブロックデータの暗号化鍵であるブロックキーが、デバイスＩＤを含むデータに基づいて生成されるとともに、デバイスＩＤが記録媒体に格納される。従って、記録媒体を再生しようとする機器は、記録媒体からデバイスＩＤを取得可能であり、同様のブロックキーを生成することが可能となるのでブロックデータの復号が可能となる。しかし、再生機器制限ありの場合は、ブロックデータの暗号化鍵であるブロックキーが、デバイス固有キーを含むデータに基づいて生成される。このデバイス固有キーはデバイス毎に異な

る秘密鍵であり、他の機器は、そのキーを取得することはできない。また、ブロックデータを暗号化して記録媒体に格納する場合、デバイス固有キーの記録媒体に対する書き込み処理は実行されない。従って、他の再生機器では、暗号化されたブロックデータを格納した記録媒体を装着しても、同一のデバイス固有キーを取得することができないので、ブロックデータを復号するための復号キーを生成することができず、復号不可能となり再生できない。なお、再生処理の詳細については後述する。

次に図２５に示すフローチャートに従って、データ記録処理に伴って実行されるＴＳ処理手段３００におけるＡＴＳ付加処理及び暗号処理手段１５０における暗号処理の処理の流れを説明する。図２５のＳ２５０１において、記録再生装置は自身のメモリ１８０に格納しているマスターキー、デバイス識別子としてのデバイスＩＤ、デバイス固有キーを読み出す。

Ｓ２５０２において、記録媒体に識別情報としてのディスクＩＤ（Disc ID）が既に記録されているかどうかを検査する。記録されていればＳ２５０３でこのディスクＩＤを読み出し、記録されていなければＳ２５０４で、ランダムに、もしくは予め定められた方法でディスクＩＤを生成し、ディスクに記録する。次に、Ｓ２５０５では、マスターキーとディスクＩＤを用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1で定められているハッシュ関数SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法などを適用することで求める。

次にＳ２５０６に進み、その一回の記録毎の固有の鍵としてのタイトルキー（Title Key）、再生機器制限フラグ（Player Restriction Flag）、さらに、機器識別情報としてのデバイスＩＤを取り出してディスクに記録する。次にＳ２５０７で、上記のディスク固有キーとタイトルキーと、デバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）から、タイトル固有キーを生成する。

タイトル固有キーの生成の詳細フローを図２７に示す。暗号処理手段１５０は、ステップＳ２７０１において、再生機器制限をするかしないかの判定を実行する。この判定は、記録再生器を使用するユーザによって入力された指示データ、ある

いはコンテンツに付加された利用制限情報に基づいて判定する。

Ｓ２７０１の判定がＮｏ、即ち、再生機器制限をしない場合は、ステップＳ２７０２に進み、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイスＩＤとから、タイトル固有キー（Title Unique Key）を生成する。

Ｓ２７０１の判定がＹｅｓ、即ち、再生機器制限をする場合は、ステップＳ２７０３に進みディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイス固有キーとから、タイトル固有キー（Title Unique Key）を生成する。キー生成には、SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する。

Ｓ２５０８では、記録再生装置は記録すべきコンテンツデータの被暗号化データをＴＳパケットの形で受信する。Ｓ２５０９で、ＴＳ処理手段３００は、各ＴＳパケットを受信した時刻情報であるＡＴＳを付加する。あるいはコピー制御情報ＣＣＩとＡＴＳ、さらに他の情報を組み合わせた値を付加する。次に、Ｓ２５１０で、ＡＴＳを付加したＴＳパケットを順次受信し、１ブロックを形成する例えばＸ＝３２に達したか、あるいはパケットの終了を示す識別データを受信したかを判定する。いずれかの条件が満足された場合はステップＳ２５１１に進み、Ｘ個、あるいはパケット終了までのパケットを並べて、１ブロックのブロックデータを形成する。

次に、暗号処理手段１５０は、Ｓ２５１２で、ブロックデータの先頭の３２ビット（ＡＴＳを含むブロック・シード）とＳ２５０７で生成したタイトル固有キーとから、そのブロックのデータを暗号化する鍵であるブロックキーを生成する。

Ｓ２５１３では、ブロックキーを用いてＳ２５１１で形成したブロックデータを暗号化する。なお、先にも説明したように、暗号化の対象となるのは、ブロックデータのｍ＋１バイト目から最終データまでである。暗号化アルゴリズムは、例えばFIPS 46-2で規定されるＤＥＳ（Data Encryption Standard）が適用される。

Ｓ２５１４で、暗号化したブロックデータを記録媒体に記録する。Ｓ２５１５で、全データを記録したかを判断する。全データを記録していれば、記録処理を終了し、全データを記録していなければＳ２５０８に戻って残りのデータの処理

を実行する。

［記録されたデータ再生についての機器制限の設定が可能なシステムにおけるデータ復号及び再生処理］

次に、上記のようにして記録媒体に記録された暗号化コンテンツを復号して再生する処理について図２９の処理ブロック図と、図３０のフローチャートを用いて説明する。

まず、図２９に示す処理ブロック図に従って説明する。記録再生装置２９００はディスク２９２０からディスクＩＤ２９０２を、また自身のメモリからマスターキー２９０１、デバイス識別子としてのデバイスＩＤ２９３１、デバイス固有キー２９３２を読み出す。先の記録処理の説明から明らかなように、ディスクＩＤはディスクに記録されているか、記録されていない場合は記録再生器において生成してディスクに記録したディスク固有の識別子である。マスターキー２９０１は、ライセンスを受けた記録再生装置に格納された秘密キーであり、デバイスＩＤは記録再生装置２９００固有の識別子、デバイス固有キーは、その記録再生器に固有の秘密鍵である。

記録再生装置２９００は、次に、ディスクＩＤ（Disc ID）とマスターキー（Master Key）を用いてディスク固有キー（Disc Unique Key）を生成２９０３する。このキー生成方法は、例えば、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクＩＤ（Disc ID）とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみをディスク固有キー（Disc Unique Key）として使用する方法や、ブロック暗号関数を用いたハッシュ関数にマスターキー（Master Key）とディスクＩＤ（Disc ID）を入力して得られた結果を用いるなどの方法が挙げられる。

次に、ディスクから読み出すべきデータに対応して記録されたタイトルキー（Title Key）２９０５を読み出し、さらに、このデータを記録した記録再生器のデバイスＩＤ２９３５と、データに対応して設定された再生機器制限フラグ２９３４を読み出し、読み出した再生機器制限フラグ２９３３が示す再生機器制限情報が、「再生機器制限あり」かつ、「記録媒体から読み出したデバイスＩＤ２９３５と自己のデバイスＩＤ２９３１が一致する」か、あるいは、読み出した再生

機器制限フラグ２９３３が示す再生機器制限情報が、「再生機器制限なし」である場合は、再生可能となり、読み出した再生機器制限フラグ２９３３が示す再生機器制限情報が、「再生機器制限あり」かつ、「記録媒体から読み出したデバイスＩＤ２９３４と自己のデバイスＩＤ２９３１が一致しない」場合は、再生不可能となる。

再生不可能とされる場合は、データは、そのデータを記録した記録再生器固有のデバイス固有キーに基づいて生成されたブロックキーによって暗号化されており、そのデータを記録した記録再生器以外の記録再生器は同一のデバイス固有キーを保有しないので、データを復号するためのブロックキーを生成することができない場合である。

再生可能である場合は、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイスＩＤ、あるいは、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイス固有キー、いずれかの組合せから、タイトル固有キー（Title Unique Key）を生成する。

即ち、再生機器制限をしない設定である場合には、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイスＩＤとからタイトル固有キー（Title Unique Key）を生成し、再生機器制限をする設定である場合には、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、自己のデバイス固有キーとからタイトル固有キー（Title Unique Key）を生成する。このキー生成方法としては、ハッシュ関数SHA-1、ブロック暗号関数を用いたハッシュ関数の適用が可能である。

なお、上記の説明では、マスターキー（Master Key）とディスクＩＤ（Disc ID）からディスク固有キー（Disc Unique Key）を生成し、これとタイトルキー（Title Key）とデバイスＩＤ、もしくはタイトルキー（Title Key）とデバイス固有キーからタイトル固有キー（Title Unique Key）をそれぞれ生成するようにしているが、ディスク固有キー（Disc Unique Key）を不要としてマスターキー（Master Key）とディスクＩＤ（Disc ID）とタイトルキー（Title Key）と、デバイスＩＤもしくはデバイス固有キーから直接タイトル固有キー（Title Unique Key）を生成してもよく、また、タイトルキー（Title Key）を用いずに、マスタ

ーキー（Master Key）とディスクＩＤ（Disc ID）と、デバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）からタイトル固有キー（Title Unique Key）相当の鍵を生成してもよい。

次にディスクに格納されている暗号化コンテンツ２９１２から順次ブロックデータ（Block Data）を読み出し、ブロックデータ（Block Data）の先頭の４バイトを構成するブロック・シード（Block Seed）をセレクタ２９１０において分離して、タイトル固有キー（Title Unique Key）との相互処理により、ブロックキー（Block Key）を生成する。

ブロック・キー（Block Key）の生成方法は、先に説明した図１４の構成を適用することができる。即ち、３２ビットのブロック・シード（Block Seed）と、６４ビットのタイトル固有キー（Title Unique Key）とから、６４ビットのブロックキー（Block Key）を生成する構成が適用できる。

なお、上記ではディスク固有キー（Disc Unique key）、タイトル固有キー（Title Unique Key）、ブロックキー（Block Key）をそれぞれ生成する例を説明したが、例えば、ディスク固有キー（Disc Unique Key）とタイトル固有キー（Title Unique Key）の生成を実行することなく、ブロック毎にマスターキー（Master Key）とディスクＩＤ（Disc ID）とタイトルキー（Title Key）と、ブロックシード（Block Seed）と、デバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）を用いてブロックキー（Block Key）を生成してもよい。

ブロックキーが生成されると、ブロックキー（Block Key）を用いて暗号化されているブロックデータを復号２９０９し、セレクタ２９０８を介して復号データとして出力する。なお、復号データには、トランスポートストリームを構成する各トランスポートパケットにＡＴＳが付加されており、先に説明したＴＳ処理手段３００において、ＡＴＳに基づくストリーム処理が実行される。その後、データは、使用、例えば、画像を表示したり、音楽を鳴らしたりすることが可能となる。

このように、ブロック単位で暗号化され記録媒体に格納された暗号化コンテンツはブロック単位でＡＴＳを含むブロック・シードに基づいて生成されるブロッ

ク鍵で復号処理が施されて再生が可能となる。

次に図３０に示すフローチャートに従って、復号処理及び再生処理について、処理の流れを説明する。図３０のＳ３００１において、記録再生装置はディスクからディスクＩＤを、また自身のメモリからマスターキー、デバイスＩＤ、デバイス固有キーを読み出す。Ｓ３００２で、ディスクＩＤとマスターキーを用いてディスク固有キーを生成する。

次にＳ３００３で、ディスクから読み出すべきデータのタイトルキー、さらに、このデータを記録した記録再生器のデバイスＩＤと、データに対応して設定された再生機器制限フラグを読み出す。

次に、Ｓ３００４で読み出すべきデータが再生可能か否かを判定する。判定の詳細を図３１に示す。図３１のステップＳ３１０１では、読み出した再生機器制限フラグの示す再生機器制限情報が、「再生機器制限あり」の設定であるか否かを判定する。ありの場合は、ステップＳ３１０２において、「記録媒体から読み出したデバイスＩＤと自己のデバイスＩＤが一致するか否か」を判定する。一致する場合は、再生可能と判定する。ステップＳ３１０１において、「再生機器制限あり」の設定でないと判定された場合も、再生可能と判定する。読み出した再生機器制限フラグが示す再生機器制限情報が、「再生機器制限あり」かつ、「記録媒体から読み出したデバイスＩＤと自己のデバイスＩＤが一致しない」場合は、再生不可能と判定する。

次に、Ｓ３００５で、タイトル固有キーの生成を行う。タイトル固有キーの生成の詳細フローを図３２に示す。暗号処理手段１５０は、ステップＳ３２０１において、再生機器制限をするの設定であるか、しないの設定であるかの判定を実行する。この判定は、ディスクから読み出した再生機器制限フラグに基づいて実行される。

Ｓ３２０１の判定がＮｏ、即ち、再生機器制限をしない設定である場合は、ステップＳ３２０２に進み、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイスＩＤとから、タイトル固有キー（Title Unique Key）を生成する。

Ｓ３２０１の判定がＹｅｓ、即ち、再生機器制限をする場合は、ステップＳ３

２０３に進みディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、自己の記録再生器の有するデバイス固有キーとから、タイトル固有キー（Title Unique Key）を生成する。キー生成には、SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する。

次にＳ３００６でディスクから暗号化されて格納されているブロックデータを読み出す。Ｓ３００７で、ブロックデータの先頭の４バイトのブロックシード（Block Seed）と、Ｓ３００５で生成したタイトル固有キーを用いてブロックキーを生成する。

次に、Ｓ３００８で、ブロックキーを用いて暗号化されているブロックデータを復号し、Ｓ３００９で、全データを読み出したかを判断し、全データを読み出していれば終了し、そうでなければＳ３００６に戻り残りのデータを読み出す。

以上のように、再生機器制限をしない場合は、デバイスＩＤに基づいてブロックキーを生成し、再生機器制限をする場合は、デバイス固有キーに基づいてブロックキーを生成するという２つの設定が可能であり、いずれかの設定に基づいてコンテンツをブロック単位で暗号化して記録媒体に格納することができる。記録媒体に格納されたデータを再生する場合、デバイス固有キーに基づいて暗号化されたデータに関しては、そのデータを記録した機器でのみ再生可能とする構成となり、再生機器制限をしない場合は、ディスクに記録したデバイスＩＤを用いて他の機器がブロックキーを生成することが可能となるので他の機器における復号処理、再生処理を実行を可能とすることができる。

［記録処理におけるコピー制御］

さて、コンテンツの著作権者等の利益を保護するには、ライセンスを受けた装置において、コンテンツのコピーを制御する必要がある。

即ち、コンテンツを記録媒体に記録する場合には、そのコンテンツが、コピーしてもよいもの（コピー可能）かどうかを調査し、コピーして良いコンテンツだけを記録するようにする必要がある。また、記録媒体に記録されたコンテンツを再生して出力する場合には、その出力するコンテンツが、後で、違法コピーされないようにする必要がある。

そこで、そのようなコンテンツのコピー制御を行いながら、コンテンツの記録

再生を行う場合の図１又は図２の記録再生装置の処理について、図３３及び図３４のフローチャートを参照して説明する。

まず、外部からのディジタル信号のコンテンツを、記録媒体に記録する場合においては、図３３（Ａ）のフローチャートに従った記録処理が行われる。図３３（Ａ）の処理について説明する。図１の記録再生器１００を例として説明する。ディジタル信号のコンテンツ（ディジタルコンテンツ）が、例えば、IEEE1394シリアルバス等を介して、入出力Ｉ／Ｆ１２０に供給されると、ステップＳ３３０１において、入出力Ｉ／Ｆ１２０は、そのディジタルコンテンツを受信し、ステップＳ３３０２に進む。

ステップＳ３３０２では、入出力Ｉ／Ｆ１２０は、受信したディジタルコンテンツが、コピー可能であるかどうかを判定する。即ち、例えば、入出力Ｉ／Ｆ１２０が受信したコンテンツが暗号化されていない場合（例えば、上述のＤＴＣＰを使用せずに、平文のコンテンツが、入出力Ｉ／Ｆ１２０に供給された場合）には、そのコンテンツは、コピー可能であると判定される。

また、記録再生装置１００がＤＴＣＰに準拠している装置であるとし、ＤＴＣＰに従って処理を実行するものとする。ＤＴＣＰでは、コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)が規定されている。ＥＭＩが００Ｂ（Ｂは、その前の値が２進数であることを表す）である場合は、コンテンツがコピーフリーのもの(Copy-freely)であることを表し、ＥＭＩが０１Ｂである場合には、コンテンツが、それ以上のコピーをすることができないもの(No-more-copies)であることを表す。さらに、ＥＭＩが１０Ｂである場合は、コンテンツが、１度だけコピーして良いもの(Copy-one-generation)であることを表し、ＥＭＩが１１Ｂである場合には、コンテンツが、コピーが禁止されているもの(Copy-never)であることを表す。

記録再生装置１００の入出力Ｉ／Ｆ１２０に供給される信号にＥＭＩが含まれ、そのＥＭＩが、Copy-freelyやCopy-one-generationであるときには、コンテンツはコピー可能であると判定される。また、ＥＭＩが、No-more-copiesやCopy-neverであるときには、コンテンツはコピー可能でないと判定される。

ステップＳ３３０２において、コンテンツがコピー可能でないと判定された場

合、ステップＳ３３０３～Ｓ３３０５をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体１９５に記録されない。

また、ステップＳ３３０２において、コンテンツがコピー可能であると判定された場合、ステップＳ３３０３に進み、以下、ステップＳ３３０３～Ｓ３３０５において、図３（Ａ）のステップＳ３０２、Ｓ３０３、Ｓ３０４における処理と同様の処理が行われる。即ち、ＴＳ処理手段３００によるトランスポートパケットに対するＡＴＳ付加、暗号処理手段Ｉ５０における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体１９５に記録して、記録処理を終了する。

なお、ＥＭＩは、入出力Ｉ／Ｆ１２０に供給されるディジタル信号に含まれるものであり、ディジタルコンテンツが記録される場合には、そのディジタルコンテンツとともに、ＥＭＩ、あるいは、ＥＭＩと同様にコピー制御状態を表す情報（例えば、ＤＴＣＰにおけるembedded CCIなど）も記録される。

この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。

本発明の記録再生装置では、このＥＭＩやembedded CCIなどのコピー制御情報を、ＴＳパケットに付加する形で記録する。即ち、図１０の例２や例３のように、ＡＴＳを２４ビット乃至３０ビット分と、コピー制御情報を加えた３２ビットを図５に示すように各ＴＳパケットに付加する。

外部からのアナログ信号のコンテンツを、記録媒体に記録する場合においては、図３３（Ｂ）のフローチャートに従った記録処理が行われる。図３３（Ｂ）の処理について説明する。アナログ信号のコンテンツ（アナログコンテンツ）が、入出力Ｉ／Ｆ１４０に供給されると、入出力Ｉ／Ｆ１４０は、ステップＳ３３１１において、そのアナログコンテンツを受信し、ステップＳ３３１２に進み、受信したアナログコンテンツが、コピー可能であるかどうかを判定する。

ここで、ステップＳ３３１２の判定処理は、例えば、入出力Ｉ／Ｆ１４０で受信した信号に、マクロビジョン(Macrovision)信号や、ＣＧＭＳ－Ａ(Copy Generation Management System-Analog)信号が含まれるかどうかに基づいて行われる。即ち、マクロビジョン信号は、ＶＨＳ方式のビデオカセットテープに記録すると、

ノイズとなるような信号であり、これが、入出力Ｉ／Ｆ１４０で受信した信号に含まれる場合には、アナログコンテンツは、コピー可能でないと判定される。

また、例えば、ＣＧＭＳ－Ａ信号は、ディジタル信号のコピー制御に用いられるＣＧＭＳ信号を、アナログ信号のコピー制御に適用した信号で、コンテンツがコピーフリーのもの(Copy-freely)、１度だけコピーして良いもの(Copy-one-generation)、又はコピーが禁止されているもの(Copy-never)のうちのいずれであるかを表す。

従って、ＣＧＭＳ－Ａ信号が、入出力Ｉ／Ｆ１４０で受信した信号に含まれ、かつ、そのＣＧＭＳ－Ａ信号が、Copy-freelyやCopy-one-generationを表している場合には、アナログコンテンツは、コピー可能であると判定される。また、ＣＧＭＳ－Ａ信号が、Copy-neverを表している場合には、アナログコンテンツは、コピー可能でないと判定される。

さらに、例えば、マクロビジョン信号も、ＣＧＭＳ－Ａ信号も、入出力Ｉ／Ｆ４で受信した信号に含まれない場合には、アナログコンテンツは、コピー可能であると判定される。

ステップＳ３３１２において、アナログコンテンツがコピー可能でないと判定された場合、ステップＳ３３１３乃至Ｓ３３１７をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体１９５に記録されない。

また、ステップＳ３３１２において、アナログコンテンツがコピー可能であると判定された場合、ステップＳ３３１３に進み、以下、ステップＳ３３１３乃至Ｓ３３１７において、図３（Ｂ）のステップＳ３２２乃至Ｓ３２６における処理と同様の処理が行われ、これにより、コンテンツがディジタル変換、ＭＰＥＧ符号化、ＴＳ処理、暗号化処理がなされて記録媒体に記録され、記録処理を終了する。

なお、入出力Ｉ／Ｆ１４０で受信したアナログ信号に、ＣＧＭＳ－Ａ信号が含まれている場合に、アナログコンテンツを記録媒体に記録するときには、そのＣＧＭＳ－Ａ信号も、記録媒体に記録される。即ち、図１０で示したＣＣＩもしくはその他の情報の部分に、この信号が記録される。この際、一般的には、Copy-One-generationを表す情報は、それ以上のコピーを許さないよう、No-more-copie

sに変換されて記録される。但し、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

［再生処理におけるコピー制御］

次に、記録媒体に記録されたコンテンツを再生して、ディジタルコンテンツとして外部に出力する場合においては、図３４（Ａ）のフローチャートに従った再生処理が行われる。図３４（Ａ）の処理について説明する。まず最初に、ステップＳ３４０１、Ｓ３４０２、Ｓ３４０３において、図４（Ａ）のステップＳ４０１、Ｓ４０２、Ｓ４０３における処理と同様の処理が行われ、これにより、記録媒体から読み出された暗号化コンテンツが暗号処理手段１５０において復号処理がなされ、ＴＳ処理がなされる。各処理が実行されたディジタルコンテンツは、バス１１０を介して、入出力Ｉ／Ｆ１２０に供給される。

入出力Ｉ／Ｆ１２０は、ステップＳ３４０４において、そこに供給されるディジタルコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、入出力Ｉ／Ｆ１２０に供給されるディジタルコンテンツにＥＭＩ、あるいは、ＥＭＩと同様にコピー制御状態を表す情報（コピー制御情報）が含まれない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

また、例えば、入出力Ｉ／Ｆ１２０に供給されるディジタルコンテンツにＥＭＩが含まれる場合、従って、コンテンツの記録時に、ＤＴＣＰの規格に従って、ＥＭＩが記録された場合には、そのＥＭＩ（記録されたＥＭＩ(Recorded EMI)）が、Copy-freelyであるときには、ディジタルコンテンツは、後でコピー可能なものであると判定される。また、ＥＭＩが、No-more-copiesであるときには、コンテンツは、後でコピー可能なものでないと判定される。

なお、一般的には、記録されたＥＭＩが、Copy-one-generationやCopy-neverであることはない。Copy-one-generationのＥＭＩは記録時にNo-more-copiesに変換され、また、Copy-neverのＥＭＩを持つディジタルコンテンツは、記録媒体に記録されないからである。但し、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

ステップＳ３４０４において、コンテンツが、後でコピー可能なものであると判定された場合、ステップＳ３４０５に進み、入出力Ｉ／Ｆ１２０は、そのディジタルコンテンツを、外部に出力し、再生処理を終了する。

また、ステップＳ３４０４において、コンテンツが、後でコピー可能なものでないと判定された場合、ステップＳ３４０６に進み、入出力Ｉ／Ｆ１２０は、例えば、ＤＴＣＰの規格等に従って、ディジタルコンテンツを、そのディジタルコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

即ち、例えば、上述のように、記録されたＥＭＩが、No-more-copiesである場合（もしくは、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたＥＭＩがCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

このため、入出力Ｉ／Ｆ１２０は、ＤＴＣＰの規格に従い、相手の装置との間で認証を相互に行い、相手が正当な装置である場合（ここでは、ＤＴＣＰの規格に準拠した装置である場合）には、ディジタルコンテンツを暗号化して、外部に出力する。

次に、記録媒体に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図３４（Ｂ）のフローチャートに従った再生処理が行われる。図３４（Ｂ）の処理について説明する。ステップＳ３４１１乃至Ｓ３４１５において、図４（Ｂ）のステップＳ４２１乃至Ｓ４２５における処理と同様の処理が行われる。即ち、暗号化コンテンツの読み出し、復号処理、ＴＳ処理、ＭＰＥＧデコード、Ｄ／Ａ変換が実行される。これにより得られるアナログコンテンツは、入出力Ｉ／Ｆ１４０で受信される。

入出力Ｉ／Ｆ１４０は、ステップＳ３４１６において、そこに供給されるコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、記録されていたコンテンツとともにコピー制御情報が記録されていなかった場合には、そのコンテンツは、後でコピー可能なものであると判定される。

また、コンテンツの記録時に、例えばＤＴＣＰの規格に従って、ＥＭＩ又はコピー制御情報が記録された場合には、そのＥＭＩ又はコピー制御情報が、Copy-f

reelyであるときには、コンテンツは、後でコピー可能なものであると判定される。

また、ＥＭＩ又はコピー制御情報が、No-more-copiesである場合、もしくは、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたＥＭＩ又はコピー制御情報がCopy-one-generationである場合には、コンテンツは、後でコピー可能なものでないと判定される。

さらに、例えば、入出力Ｉ／Ｆ１４０に供給されるアナログコンテンツにＣＧＭＳ－Ａ信号が含まれる場合、従って、コンテンツの記録時に、そのコンテンツとともにＣＧＭＳ－Ａ信号が記録された場合には、そのＣＧＭＳ－Ａ信号が、Copy-freelyであるときには、アナログコンテンツは、後でコピー可能なものであると判定される。また、ＣＧＭＳ－Ａ信号が、Copy-neverであるときには、アナログコンテンツは、後でコピー可能なものでないと判定される。

ステップＳ３４１６において、アナログコンテンツが、後でコピー可能であると判定された場合、ステップＳ３４１７に進み、入出力Ｉ／Ｆ１４０は、そこに供給されたアナログ信号を、そのまま外部に出力し、再生処理を終了する。

また、ステップＳ３４１６において、アナログコンテンツが、後でコピー可能でないと判定された場合、ステップＳ３４１８に進み、入出力Ｉ／Ｆ１４０は、アナログコンテンツを、そのアナログコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

即ち、例えば、上述のように、記録されたＥＭＩ等のコピー制御情報が、No-more-copiesである場合（もしくは、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたＥＭＩ等のコピー制御情報がCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

このため、入出力Ｉ／Ｆ１４０は、アナログコンテンツを、それに、例えば、マクロビジョン信号や、Copy-neverを表すＧＣＭＳ－Ａ信号を付加して、外部に出力する。また、例えば、記録されたＣＧＭＳ－Ａ信号が、Copy-neverである場

合にも、コンテンツは、それ以上のコピーは許されない。このため、入出力Ｉ／Ｆ４は、ＣＧＭＳ－Ａ信号をCopy-neverに変更して、アナログコンテンツとともに、外部に出力する。

以上のように、コンテンツのコピー制御を行いながら、コンテンツの記録再生を行うことにより、コンテンツに許された範囲外のコピー（違法コピー）が行われることを防止することが可能となる。

［データ処理手段の構成］

なお、上述した一連の処理は、ハードウェアにより行うことは勿論、ソフトウェアにより行うこともできる。即ち、例えば、暗号処理手段１５０は暗号化／復号ＬＳＩとして構成することも可能であるが、汎用のコンピュータや、１チップのマイクロコンピュータにプログラムを実行させることにより行う構成とすることも可能である。同様にＴＳ処理手段３００も処理をソフトウェアによって実行することが可能である。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや１チップのマイクロコンピュータ等にインストールされる。図３５は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク３５０５やＲＯＭ３５０３に予め記録しておくことができる。あるいは、プログラムはフロッピーディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体３５１０に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体３５１０は、いわゆるパッケージソフトウエアとして提供することができる。

なお、プログラムは、上述したようなリムーバブル記録媒体３５１０からコンピュータにインストールする他、ダウンロードサイトから、ディジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通

信部３５０８で受信し、内蔵するハードディスク３５０５にインストールすることができる。

コンピュータは、ＣＰＵ(Central Processing Unit)３５０２を内蔵している。ＣＰＵ３５０２には、バス３５０１を介して、入出力インタフェース３５１１が接続されており、ＣＰＵ３５０２は、入出力インタフェース３５１０を介して、ユーザによって、キーボードやマウス等で構成される入力部３５０７が操作されることにより指令が入力されると、それに従って、ＲＯＭ(Read Only Memory)３５０３に格納されているプログラムを実行する。

あるいは、ＣＰＵ３５０２は、ハードディスク３５０５に格納されているプログラム、衛星もしくはネットワークから転送され、通信部３５０８で受信されてハードディスク３５０５にインストールされたプログラム、又はドライブ３５０９に装着されたリムーバブル記録媒体３５１０から読み出されてハードディスク３５０５にインストールされたプログラムを、ＲＡＭ(Random Access Memory)３５０４にロードして実行する。

これにより、ＣＰＵ３５０２は、上述したフローチャートに従った処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、ＣＰＵ３５０２は、その処理結果を、必要に応じて、例えば、入出力インタフェース３５１１を介して、ＬＣＤ(Liquid Crystal Display)やスピーカ等で構成される出力部３５０６から出力、あるいは、通信部３５０８から送信、さらには、ハードディスク３５０５に記録させる。

ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

また、プログラムは、１つのコンピュータにより処理されるものであってもよいし、複数のコンピュータによって分散処理されるものであってもよい。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであってもよい。

なお、本実施の形態では、コンテンツの暗号化／復号を行うブロックを、１チップの暗号化／復号ＬＳＩで構成する例を中心として説明したが、コンテンツの

暗号化／復号を行うブロックは、例えば、図１及び図２に示すＣＰＵ１７０が実行する１つのソフトウェアモジュールとして実現することも可能である。同様に、ＴＳ処理手段３００の処理もＣＰＵ１７０が実行する１つのソフトウェアモジュールとして実現することが可能である。

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。即ち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、特許請求の範囲の欄を参酌すべきである。

産業上の利用可能性

本発明の情報記録再生装置及び方法によれば、各パケットの着信時刻に応じたランダム性のあるデータとして構成されるＡＴＳを用いてブロック・データを暗号化するブロックキーを生成する構成としたので、ブロック毎に異なる固有キーを生成することが可能となり、ブロック毎に暗号鍵を変更でき、暗号解析に対する強度を高めることができる。また、ＡＴＳを用いてブロックキーを生成する構成とすることにより、各ブロック毎の暗号化鍵を格納するための記録媒体上の領域が不要となり、メインデータ領域が有効に使用可能となる。さらに、データの記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなり、処理が効率的になる。

請求の範囲

１．　記録媒体に情報を記録する情報記録装置において、

間欠的なトランスポートパケットからなるトランスポートストリームを構成する各パケットに受信時刻情報（ＡＴＳ）を付加するトランスポート・ストリーム処理手段と、

前記受信時刻情報（ＡＴＳ）の付加された１以上のパケットからなるブロックデータに対する暗号処理用のブロックキーを前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の暗号処理を実行する暗号処理手段と、を有し、

前記暗号処理手段によって暗号化したデータを前記記録媒体に記録する構成としたことを特徴とする情報記録装置。

２．　前記暗号処理手段は、

前記ブロックデータを構成する複数のトランスポートパケットの先頭のトランスポートパケットに付加された受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードに基づいて、前記ブロックデータに対する暗号処理用のブロックキーを生成する構成であることを特徴とする請求の範囲第１項に記載の情報記録装置。

３．　前記暗号処理手段は、

情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、該タイトル固有キーと前記ブロックシードに基づいてブロックキーを生成する構成であることを特徴とする請求の範囲第１項に記載の情報記録装置。

４．　前記暗号処理手段は、

記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとを生成して前記記録媒体に格納する処理を実行

する構成を有することを特徴とする請求の範囲第１項に記載の情報記録装置。

５．　前記ブロックシードは、

前記受信時刻情報（ＡＴＳ）の他にコピー制御情報を含むデータであることを特徴とする請求の範囲第１項に記載の情報記録装置。

６．　前記暗号処理手段は、

前記ブロックデータの暗号処理において、該ブロックデータのブロックシードを含む先頭領域データ以外のブロックデータ構成データのみを前記ブロックキーにより暗号化する構成であることを特徴とする請求の範囲第１項に記載の情報記録装置。

７．　前記暗号処理手段は、

情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーを暗号関数の鍵とし、前記ブロックシードを前記暗号関数に入力して暗号化した結果をブロックキーとして出力する構成であることを特徴とする請求の範囲第１項に記載の情報記録装置。

８．　前記暗号処理手段は、

情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーと、前記ブロックシードとを一方向関数に入力して暗号化した結果をブロックキーとして出力する構成であることを特徴とする請求の範囲第１項に記載の情報記録装置。

９．　前記暗号処理手段は、

該暗号処理手段を構成するＬＳＩに格納されたＬＳＩキー、前記情報記録装置に格納されたデバイスキー、前記記録媒体に格納されたメディアキー、前記記録媒体のドライブ装置に格納されたドライブキーのいずれか、又はこれら各キーの組合わせに基づいてデバイス固有キーを生成し、生成したデバイス固有キーと前記ブロックシードとに基づいて前記ブロックデータに対する暗号処理用のブロックキーを生成する構成であることを特徴とする請求の範囲第１項に記載の情報記

録装置。

１０．　前記暗号処理手段は、

前記ブロックデータに対するブロックキーによる暗号処理をＤＥＳアルゴリズムに従って実行する構成であることを特徴とする請求の範囲第１項に記載の情報記録装置。

１１．　前記情報記録装置は、

記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、

前記インタフェース手段は、前記トランスポートストリームを構成する各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に対する記録実行の可否を制御する構成を有することを特徴とする請求の範囲第１項に記載の情報記録装置。

１２．　前記情報記録装置は、

記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、

前記インタフェース手段は、コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)を識別し、該ＥＭＩに基づいて記録媒体に対する記録実行の可否を制御する構成を有することを特徴とする請求の範囲第１項に記載の情報記録装置。

１３．　記録媒体から情報を再生する情報再生装置において、

前記記録媒体に記録された暗号データを復号する暗号処理手段であり、

複数のトランスポートパケットの各々に受信時刻情報（ＡＴＳ）を付加したブロックデータの暗号化データに対する復号処理用のブロックキーを前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の復号処理を実行する暗号処理手段と、

前記暗号処理手段において復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報（ＡＴＳ）に基づいてデータ出力制御を実行するトランスポート・ストリーム処理手段と、

を有することを特徴とする情報再生装置。

１４．　前記暗号処理手段は、

前記ブロックデータを構成する複数のトランスポートパケットの先頭のトランスポートパケットに付加された受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードに基づいて、前記ブロックデータに対する復号処理用のブロックキーを生成する構成であることを特徴とする請求の範囲第１３項に記載の情報再生装置。

１５．　前記暗号処理手段は、

情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、該タイトル固有キーと前記ブロックシードに基づいてブロックキーを生成する構成であることを特徴とする請求の範囲第１３項に記載の情報再生装置。

１６．　前記ブロックシードは、

前記受信時刻情報（ＡＴＳ）の他にコピー制御情報を含むデータであることを特徴とする請求の範囲第１３項に記載の情報再生装置。

１７．　前記暗号処理手段は、

前記ブロックデータの復号処理において、該ブロックデータのブロックシードを含む先頭領域データ以外のブロックデータ構成データのみを前記ブロックキーにより復号する構成であることを特徴とする請求の範囲第１３項に記載の情報再生装置。

１８．　前記暗号処理手段は、

情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーを暗号関数の鍵とし、前記ブロックシードを前記暗号関数に入力して暗号化した結果をブロックキーとして出力する構成であることを特徴とする請求の範囲第１３項に記載の情報再生装置。

１９．　前記暗号処理手段は、

情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとに

基づいてタイトル固有キーを生成し、生成したタイトル固有キーと、前記ブロックシードとを一方向関数に入力して暗号化した結果をブロックキーとして出力する構成であることを特徴とする請求の範囲第１３項に記載の情報再生装置。

２０．　前記暗号処理手段は、

該暗号処理手段を構成するＬＳＩに格納されたＬＳＩキー、前記情報記録装置に格納されたデバイスキー、前記記録媒体に格納されたメディアキー、前記記録媒体のドライブ装置に格納されたドライブキーのいずれか、又はこれら各キーの組合わせに基づいてデバイス固有キーを生成し、生成したデバイス固有キーと前記ブロックシードとに基づいて前記ブロックデータに対する復号処理用のブロックキーを生成する構成であることを特徴とする請求の範囲第１３項に記載の情報再生装置。

２１．　前記暗号処理手段は、

前記ブロックデータに対するブロックキーによる復号処理をＤＥＳアルゴリズムに従って実行する構成であることを特徴とする請求の範囲第１３項に記載の情報再生装置。

２２．　前記情報再生装置は、

記録媒体からの再生対象となる情報を受信するインタフェース手段を有し、

前記インタフェース手段は、前記トランスポートストリームを構成する各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて再生実行の可否を制御する構成を有することを特徴とする請求の範囲第１３項に記載の情報再生装置。

２３．　前記情報再生装置は、

記録媒体からの再生対象となる情報を受信するインタフェース手段を有し、

前記インタフェース手段は、コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)を識別し、該ＥＭＩに基づいて再生実行の可否を制御する構成を有することを特徴とする請求の範囲第１３項に記載の情報再生装置。

２４．　記録媒体に情報を記録する情報記録方法において、

トランスポートパケットからなるトランスポートストリームを構成する各パケ

ットに受信時刻情報（ＡＴＳ）を付加するトランスポート・ストリーム処理ステップと、

前記受信時刻情報（ＡＴＳ）の付加された１以上のパケットからなるブロックデータに対する暗号処理用のブロックキーを前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の暗号処理を実行する暗号処理ステップと、を有し、

前記暗号処理ステップによって暗号化したデータを前記記録媒体に記録することを特徴とする情報記録方法。

２５．　前記暗号処理ステップは、

前記ブロックデータを構成する複数のトランスポートパケットの先頭のトランスポートパケットに付加された受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードに基づいて、前記ブロックデータに対する暗号処理用のブロックキーを生成することを特徴とする請求の範囲第２４項に記載の情報記録方法。

２６．　前記暗号処理ステップは、

情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、該タイトル固有キーと前記ブロックシードに基づいてブロックキーを生成することを特徴とする請求の範囲第２４項に記載の情報記録方法。

２７．　前記情報記録方法は、さらに、

記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとを生成して前記記録媒体に格納する処理を実行する識別子生成ステップを有することを特徴とする請求の範囲第２４項に記載の情報記録方法。

２８．　前記暗号処理ステップは、

前記ブロックデータの暗号処理において、該ブロックデータのブロックシードを含む先頭領域データ以外のブロックデータ構成データのみを前記ブロックキー

により暗号化することを特徴とする請求の範囲第２４項に記載の情報記録方法。

２９．　前記暗号処理ステップは、

情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーを暗号関数の鍵とし、前記ブロックシードを前記暗号関数に入力して暗号化した結果をブロックキーとして出力することを特徴とする請求の範囲第２４項に記載の情報記録方法。

３０．　前記暗号処理ステップは、

情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーと、前記ブロックシードとを一方向関数に入力して暗号化した結果をブロックキーとして出力することを特徴とする請求の範囲第２４項に記載の情報記録方法。

３１．　前記暗号処理ステップは、

暗号処理手段を構成するＬＳＩに格納されたＬＳＩキー、情報記録装置に格納されたデバイスキー、前記記録媒体に格納されたメディアキー、前記記録媒体のドライブ装置に格納されたドライブキーのいずれか、又はこれら各キーの組合わせに基づいてデバイス固有キーを生成し、生成したデバイス固有キーと前記ブロックシードとに基づいて前記ブロックデータに対する暗号処理用のブロックキーを生成することを特徴とする請求の範囲第２４項に記載の情報記録方法。

３２．　前記暗号処理ステップは、

前記ブロックデータに対するブロックキーによる暗号処理をＤＥＳアルゴリズムに従って実行することを特徴とする請求の範囲第２４項に記載の情報記録方法。

３３．　前記情報記録方法は、さらに、

前記トランスポートストリームを構成する各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に対する記録実行の可否を制御するコピー制御ステップを有することを特徴とする請求の範囲第２４項に記載の情報記録方法。

３４．　前記情報記録方法は、さらに、

コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)を識別し、該ＥＭＩに基づいて記録媒体に対する記録実行の可否を制御するコピー制御ステップを有することを特徴とする請求の範囲第２４項に記載の情報記録方法。

３５．　記録媒体から情報を再生する情報再生方法において、

複数のトランスポートパケットの各々に受信時刻情報（ＡＴＳ）を付加したブロックデータの暗号化データに対する復号処理用のブロックキーを前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の復号処理を実行する復号処理ステップと、

前記暗号処理ステップにおいて復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報（ＡＴＳ）に基づいてデータ出力制御を実行するトランスポート・ストリーム処理ステップと、

を有することを特徴とする情報再生方法。

３６．　前記復号処理ステップは、

前記ブロックデータを構成する複数のトランスポートパケットの先頭のトランスポートパケットに付加された受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードに基づいて、前記ブロックデータに対する復号処理用のブロックキーを生成することを特徴とする請求の範囲第３５項に記載の情報再生方法。

３７．　前記復号処理ステップは、

情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、該タイトル固有キーと前記ブロックシードに基づいてブロックキーを生成することを特徴とする請求の範囲第３５項に記載の情報再生方法。

３８．　前記復号処理ステップは、

前記ブロックデータの復号処理において、該ブロックデータのブロックシードを含む先頭領域データ以外のブロックデータ構成データのみを前記ブロックキー

により復号することを特徴とする請求の範囲第３５項に記載の情報再生方法。

３９．　前記復号処理ステップは、

情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーを暗号関数の鍵とし、前記ブロックシードを前記暗号関数に入力して暗号化した結果をブロックキーとして出力することを特徴とする請求の範囲第３５項に記載の情報再生方法。

４０．　前記復号処理ステップは、

情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーと、前記ブロックシードとを一方向関数に入力して暗号化した結果をブロックキーとして出力することを特徴とする請求の範囲第３５項に記載の情報再生方法。

４１．　前記復号処理ステップは、

暗号処理手段を構成するＬＳＩに格納されたＬＳＩキー、情報記録装置に格納されたデバイスキー、前記記録媒体に格納されたメディアキー、前記記録媒体のドライブ装置に格納されたドライブキーのいずれか、又はこれら各キーの組合わせに基づいてデバイス固有キーを生成し、生成したデバイス固有キーと前記ブロックシードとに基づいて前記ブロックデータに対する復号処理用のブロックキーを生成することを特徴とする請求の範囲第３５項に記載の情報再生方法。

４２．　前記復号処理ステップは、

前記ブロックデータに対するブロックキーによる復号処理をＤＥＳアルゴリズムに従って実行することを特徴とする請求の範囲第３５項に記載の情報再生方法。

４３．　前記情報再生方法は、さらに、

前記トランスポートストリームを構成する各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体からの情報再生実行の可否を制御するコピー制御ステップを有することを特徴とする請求の範囲第３５項に記載の情報再生方法。

４４．　前記情報再生方法は、さらに、

コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)を識別し、該ＥＭＩに基づいて記録媒体からの情報再生実行の可否を制御するコピー制御ステップを有することを特徴とする請求の範囲第３５項に記載の情報再生方法。

４５．　トランスポートストリームを構成する各パケットに受信時刻情報（ＡＴＳ）を付加した１以上のパケットからなるブロックデータの暗号化鍵として使用されるブロックキーの生成情報となる受信時刻情報（ＡＴＳ）を含むブロックシードを有する非暗号化データ部と、

前記ブロックキーにより暗号化された暗号化データ部と、

を構成要素とするブロックデータを記録したことを特徴とする記録媒体。

４６．　記録媒体に情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

間欠的なトランスポートパケットからなるトランスポートストリームを構成する各パケットに受信時刻情報（ＡＴＳ）を付加するトランスポート・ストリーム処理ステップと、

前記受信時刻情報（ＡＴＳ）の付加された１以上のパケットからなるブロックデータに対する暗号処理用のブロックキーを前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の暗号処理を実行する暗号処理ステップと、

を有することを特徴とするプログラム提供媒体。

４７．　記録媒体から情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

複数のトランスポートパケットの各々に受信時刻情報（ＡＴＳ）を付加したブロックデータの暗号化データに対する復号処理用のブロックキーを前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の復号

処理を実行する復号処理ステップと、

前記暗号処理ステップにおいて復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報（ＡＴＳ）に基づいてデータ出力制御を実行するトランスポート・ストリーム処理ステップと、

を有することを特徴とするプログラム提供媒体。

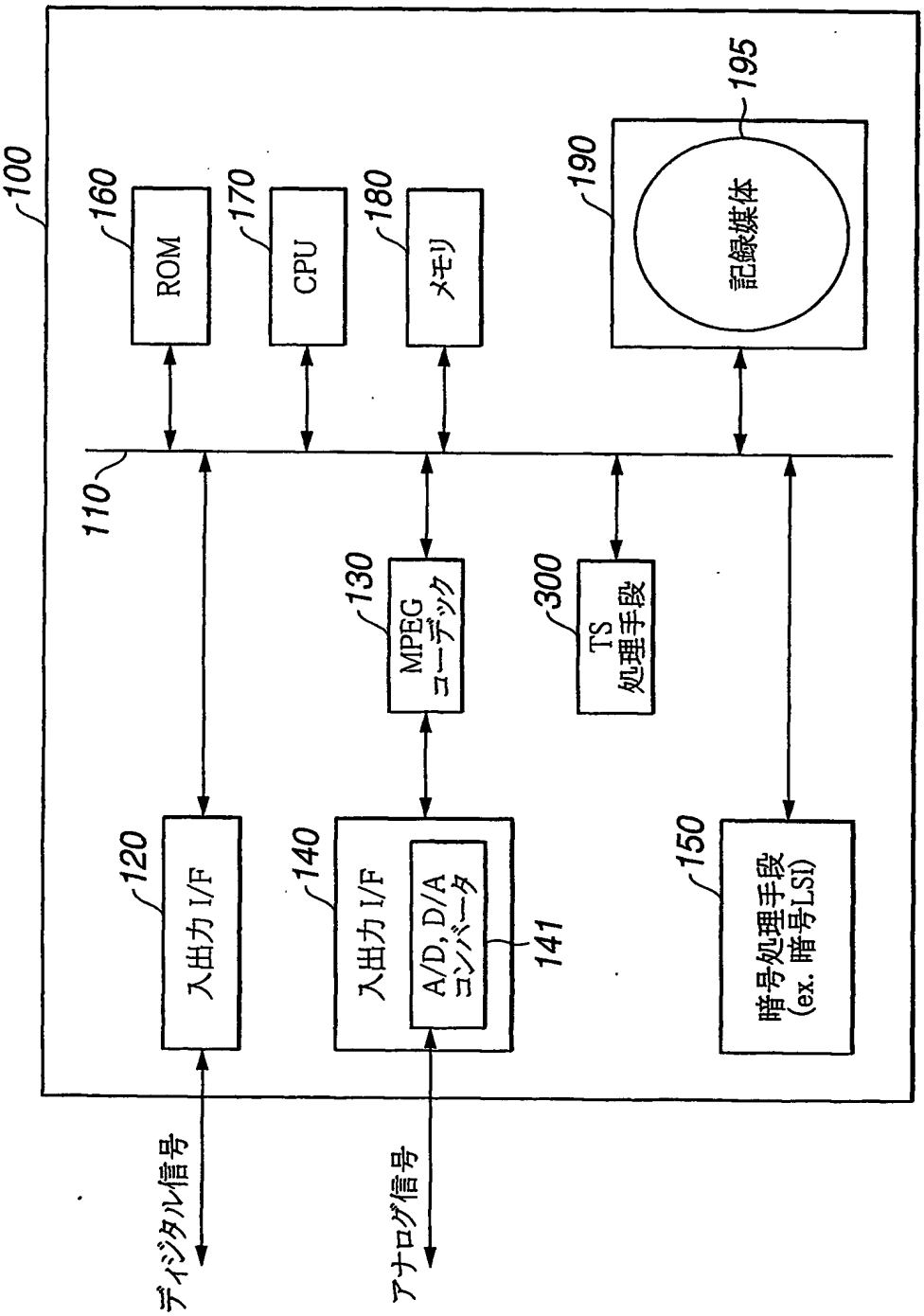

100
160
ROM
170
CPU
180
メモリ
190
195
記録媒体
110
130
MPEG
コーデック
300
TS
処理手段
120
入出力 I/F
140
入出力 I/F
A/D, D/A
コンバータ
141
150
暗号処理手段
(ex. 暗号LSI)
ディジタル信号
アナログ信号

FIG.1

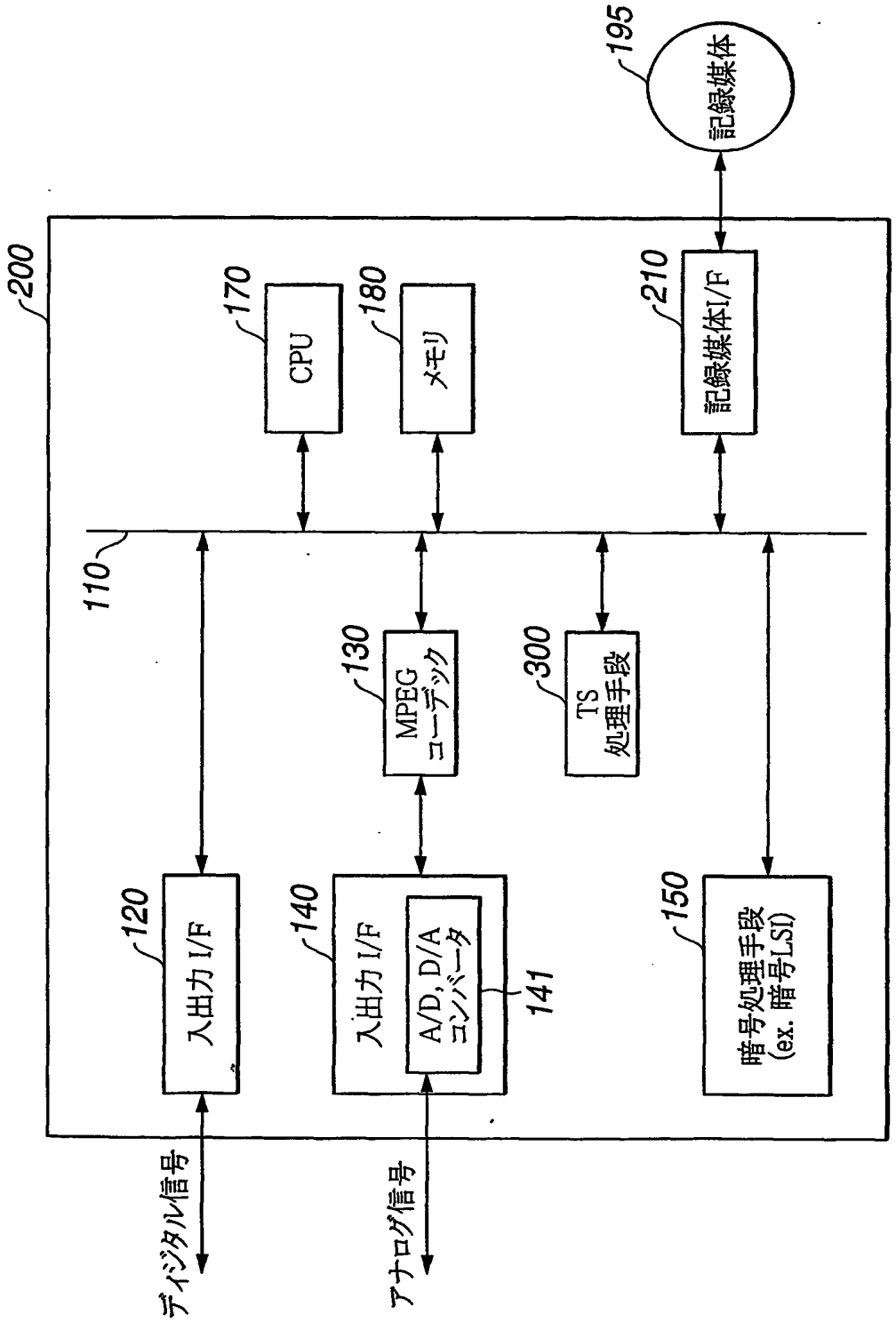

200
195
記録媒体
170
CPU
180
メモリ
210
記録媒体I/F
110
130
MPEG
コーデック
300
TS
処理手段
120
入出力 I/F
140
入出力 I/F
A/D, D/A
コンバータ
141
150
暗号処理手段
(ex. 暗号LSI)
ディジタル信号
アナログ信号

FIG.2

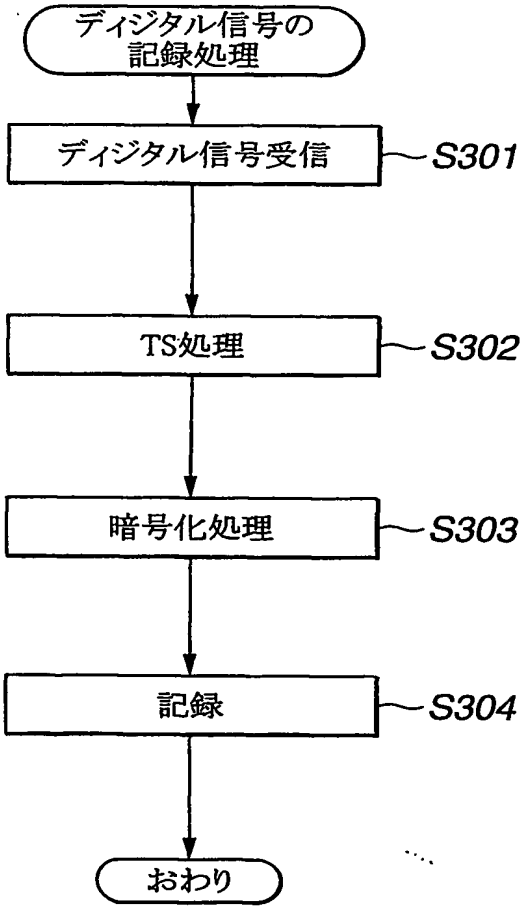

ディジタル信号の記録処理
ディジタル信号受信
S301
TS処理
S302
暗号化処理
S303
記録
S304
おわり

FIG.3A

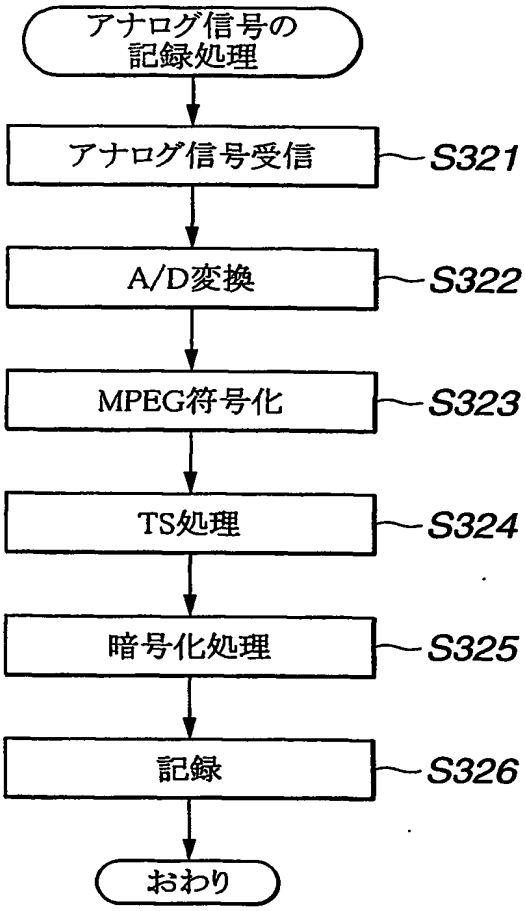

アナログ信号の記録処理
アナログ信号受信
S321
A/D変換
S322
MPEG符号化
S323
TS処理
S324
暗号化処理
S325
記録
S326
おわり

FIG.3B

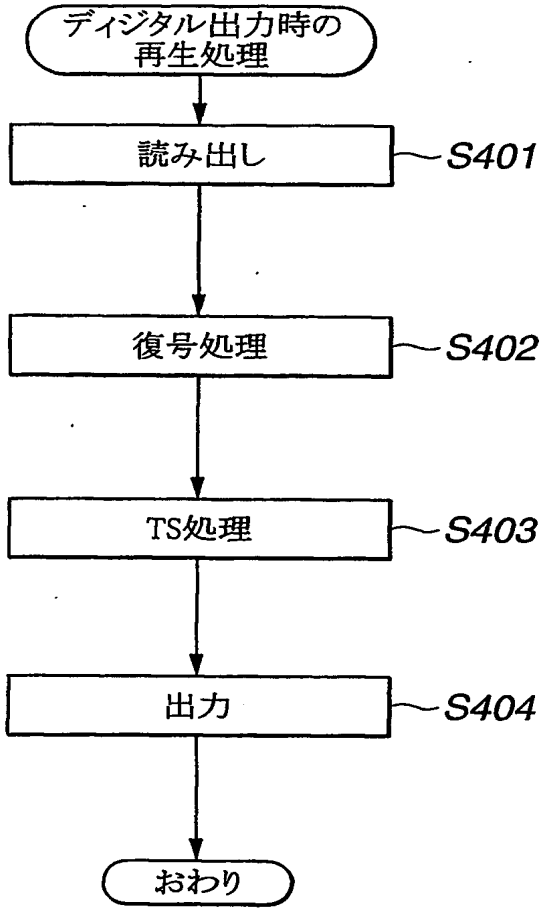

ディジタル出力時の
再生処理
読み出し
S401
復号処理
S402
TS処理
S403
出力
S404
おわり

FIG.4A

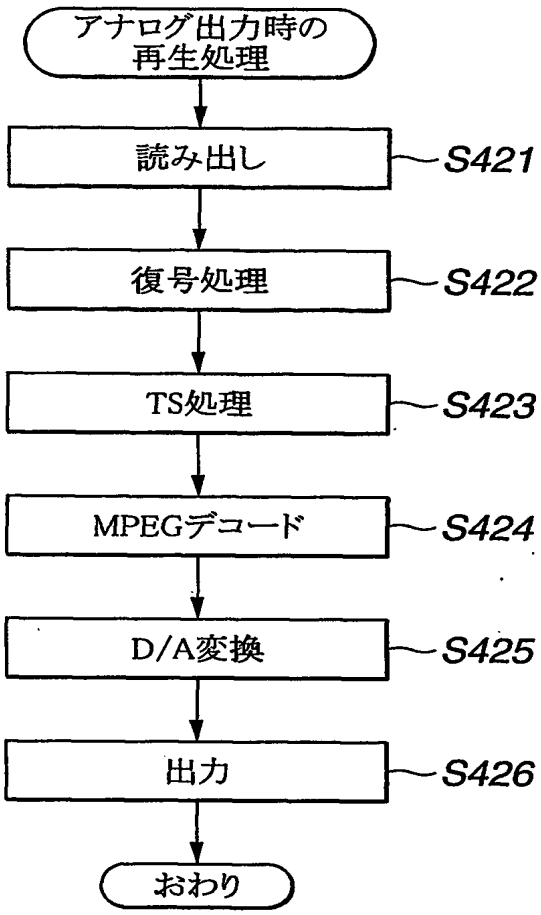

アナログ出力時の
再生処理
読み出し
S421
復号処理
S422
TS処理
S423
MPEGデコード
S424
D/A変換
S425
出力
S426
おわり

FIG.4B

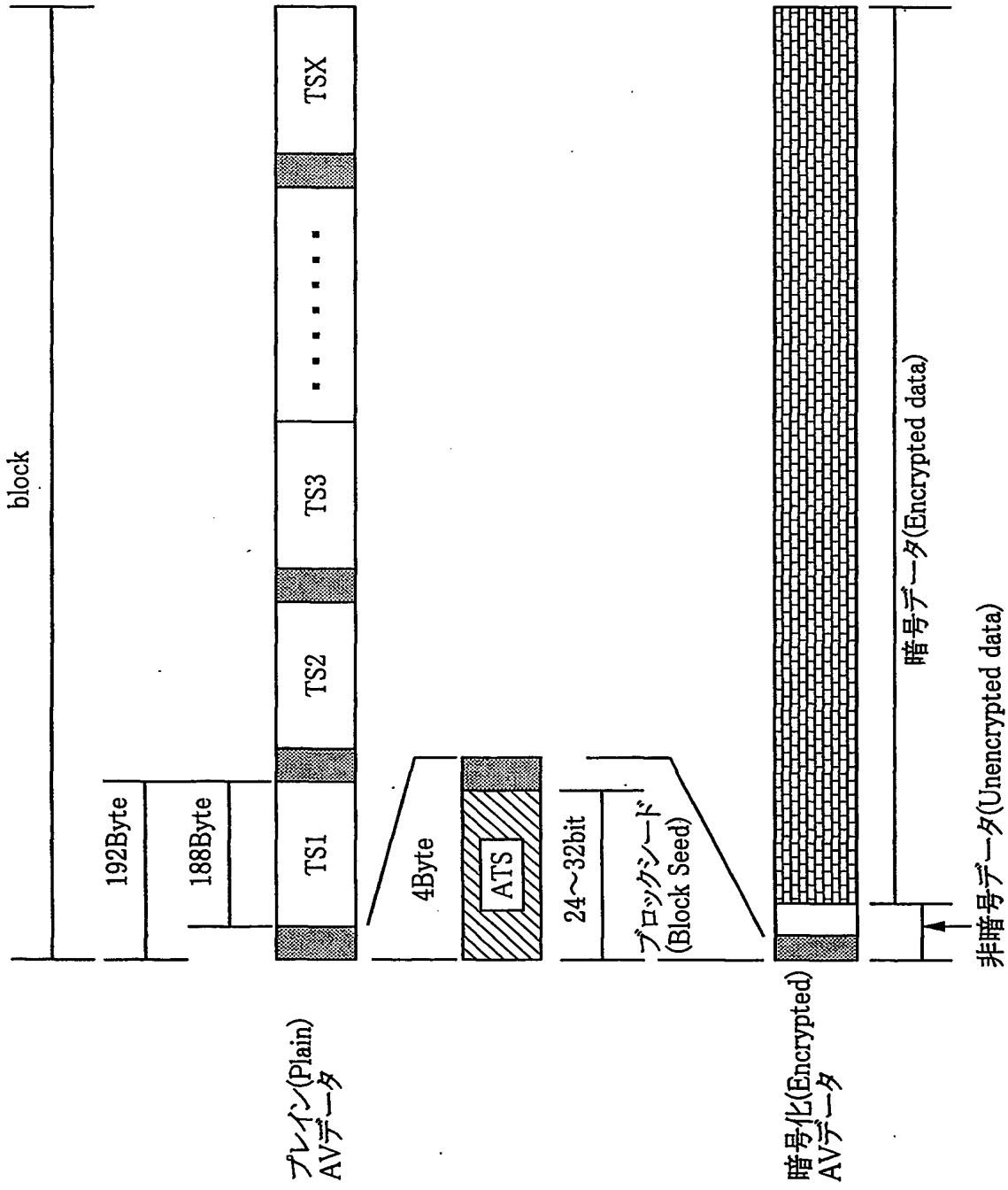

block
192Byte
188Byte
TS1
TS2
TS3
TSX
4Byte
ATS
24～32bit
ブロックシード
(Block Seed)
暗号データ(Encrypted data)
非暗号データ(Unencrypted data)
プレイン(Plain)
AVデータ
暗号化(Encrypted)
AVデータ

FIG.5

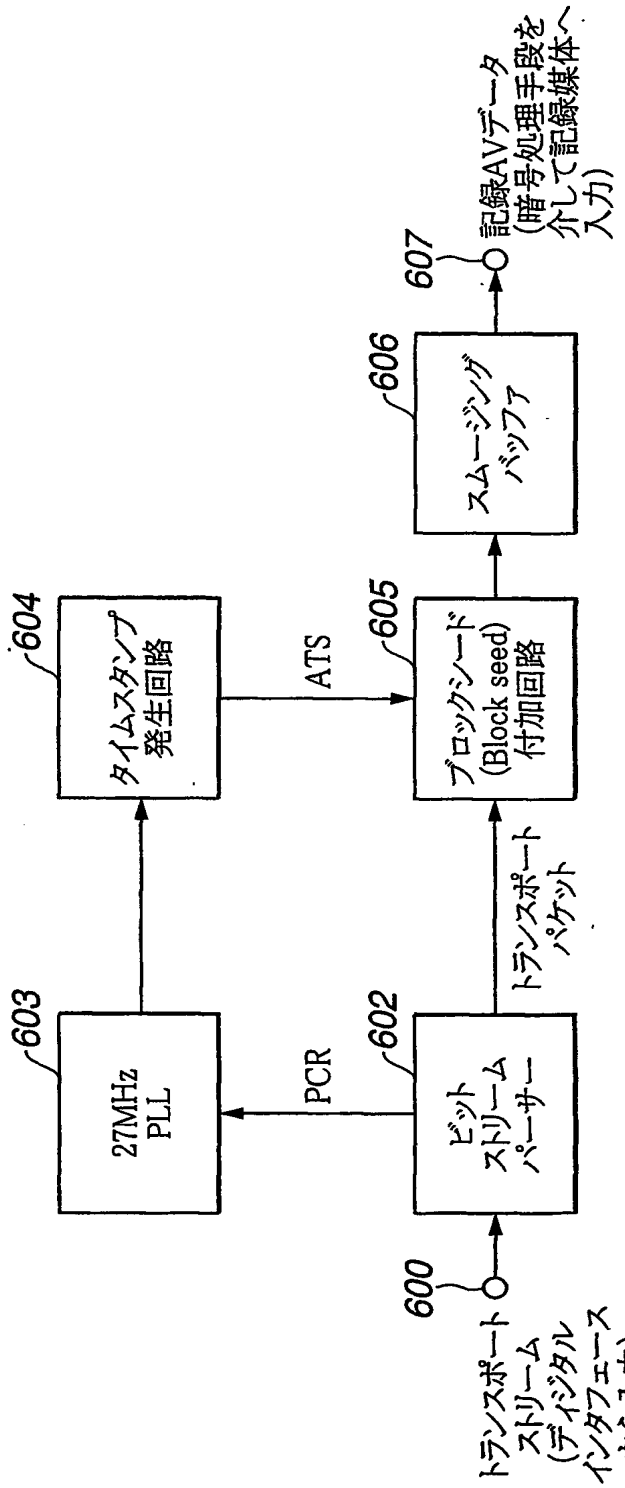

600
トランスポート
ストリーム
(デジタル
インタフェース
から入力)
602
ビット
ストリーム
パーサー
603
27MHz
PLL
PCR
トランスポート
パケット
604
タイムスタンプ
発生回路
ATS
605
ブロックシード
(Block seed)
付加回路
606
スムージング
バッファ
607
記録AVデータ
(暗号処理手段を
介して記録媒体へ
入力)

FIG.6

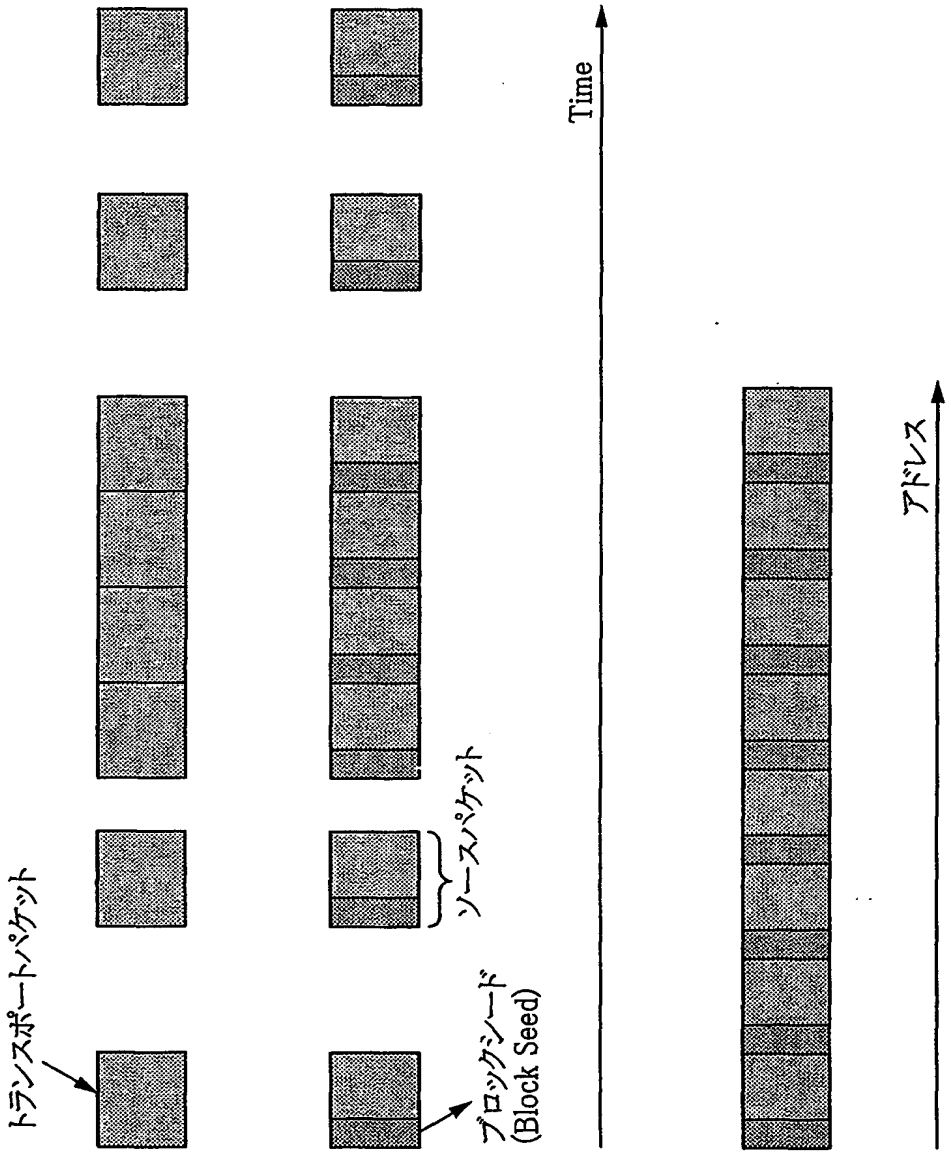


FIG.7A
入力トランスポート
ストリーム

FIG.7B
Block seed付加器
の出力

FIG.7C
記録媒体上のAV
データ

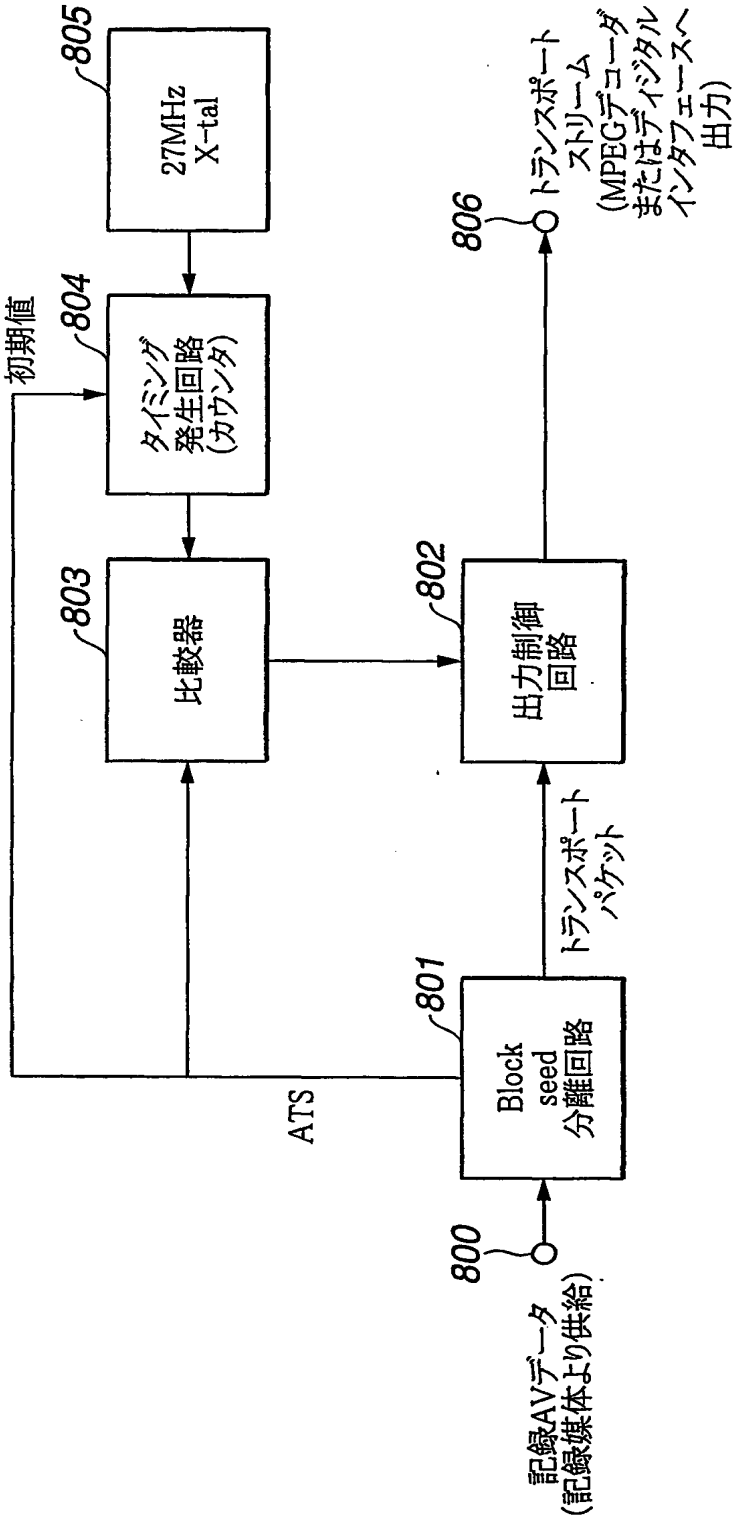

805
27MHz
X-tal
804
タイミング
発生回路
(カウンタ)
初期値
803
比較器
802
出力制御
回路
806
トランスポート
ストリーム
(MPEGデコーダ
またはディジタル
インタフェースへ
出力)
801
Block
seed
分離回路
トランスポート
パケット
ATS
800
記録AVデータ
(記録媒体より供給)

FIG.8

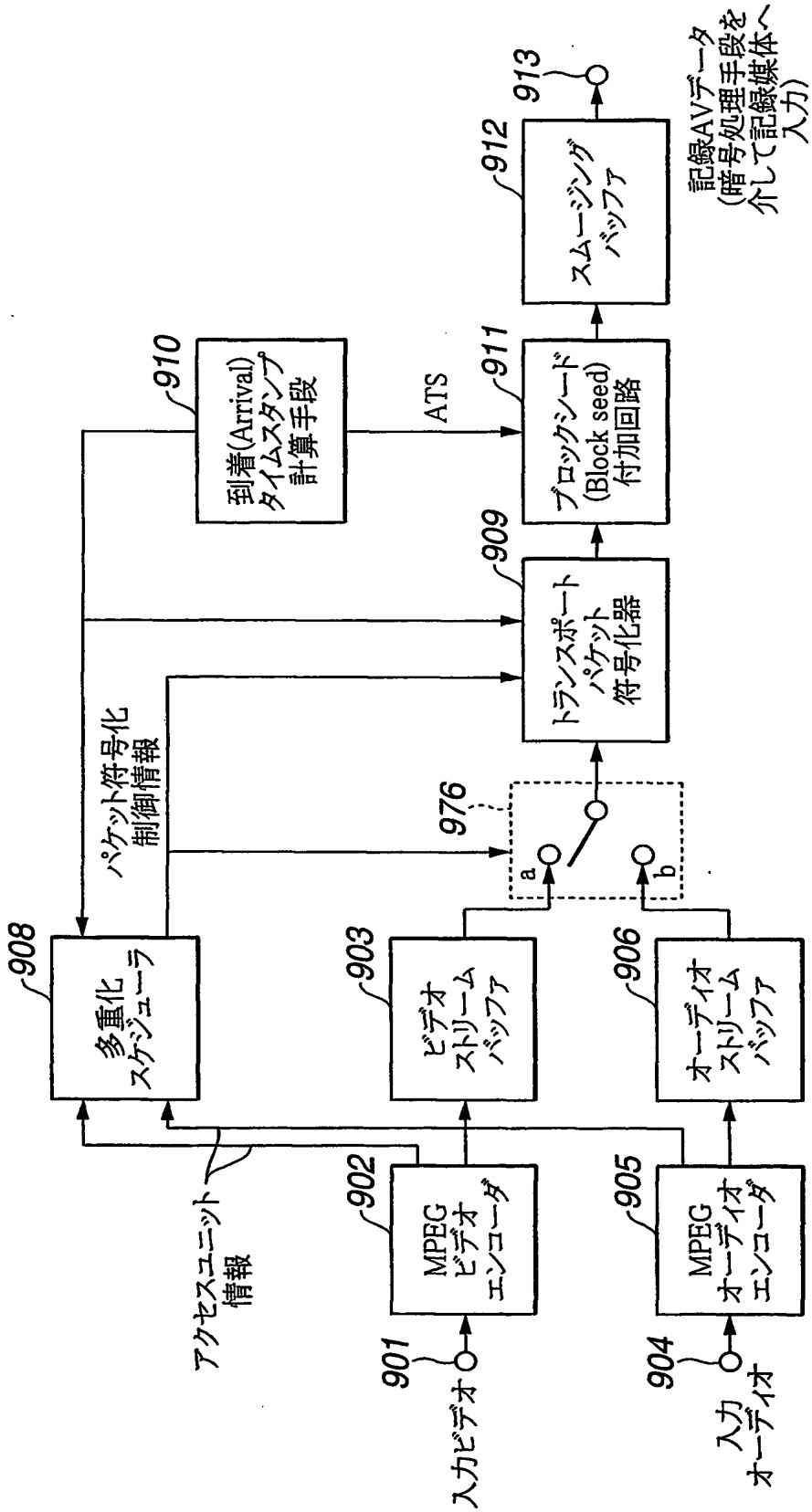

入力ビデオ
901
MPEG ビデオ エンコーダ
902
ビデオ ストリーム バッファ
903
入力 オーディオ
904
MPEG オーディオ エンコーダ
905
オーディオ ストリーム バッファ
906
アクセスユニット 情報
多重化 スケジューラ
908
パケット符号化 制御情報
トランスポート パケット 符号化器
909
976
a
b
到着(Arrival) タイムスタンプ 計算手段
910
ATS
ブロックシード (Block seed) 付加回路
911
スムージング バッファ
912
913
記録AVデータ (暗号処理手段を 介して記録媒体へ 入力)

FIG.9

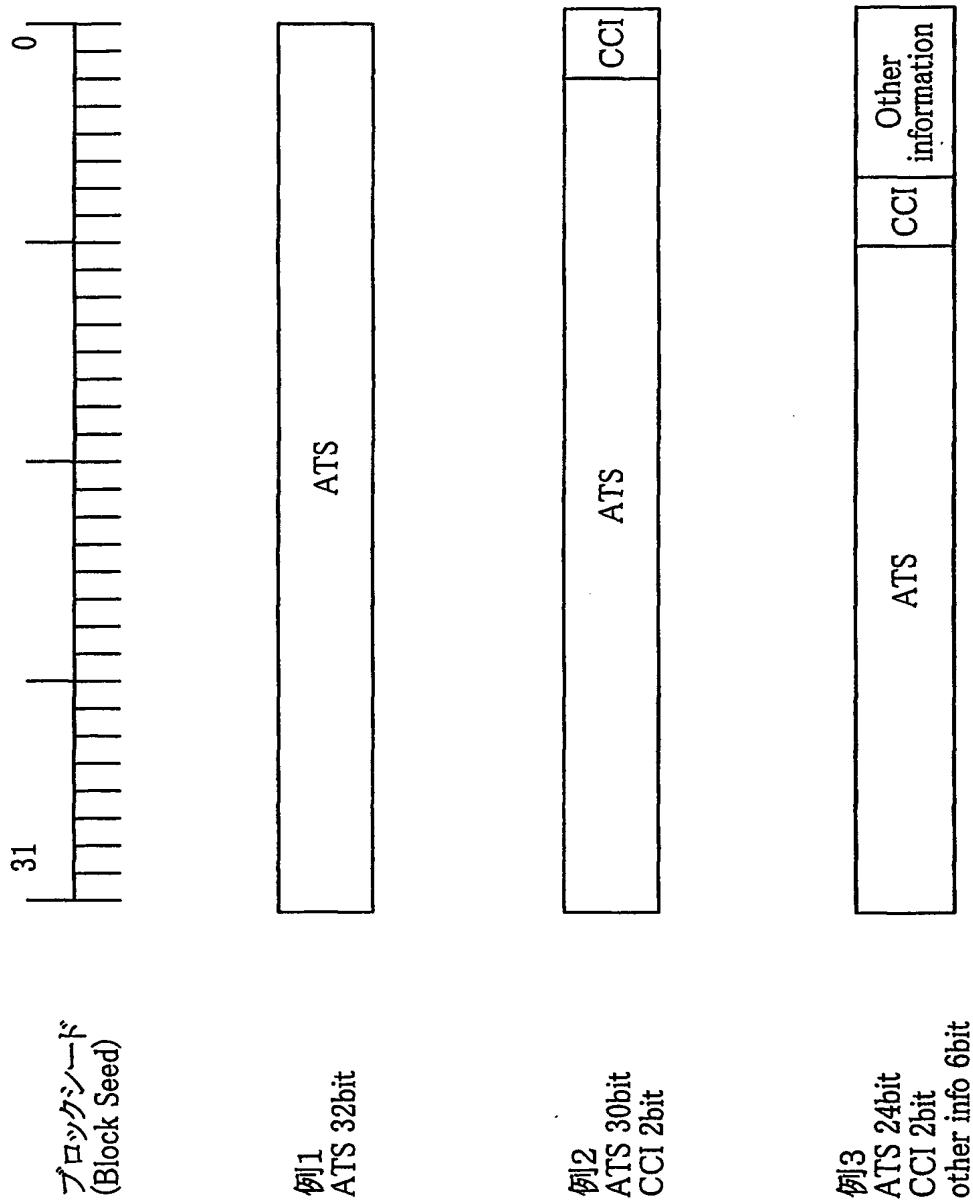

31
0
ブロックシード
(Block Seed)
例1
ATS 32bit
ATS
例2
ATS 30bit
CCI 2bit
ATS
CCI
例3
ATS 24bit
CCI 2bit
other info 6bit
ATS
CCI
Other information

FIG.10

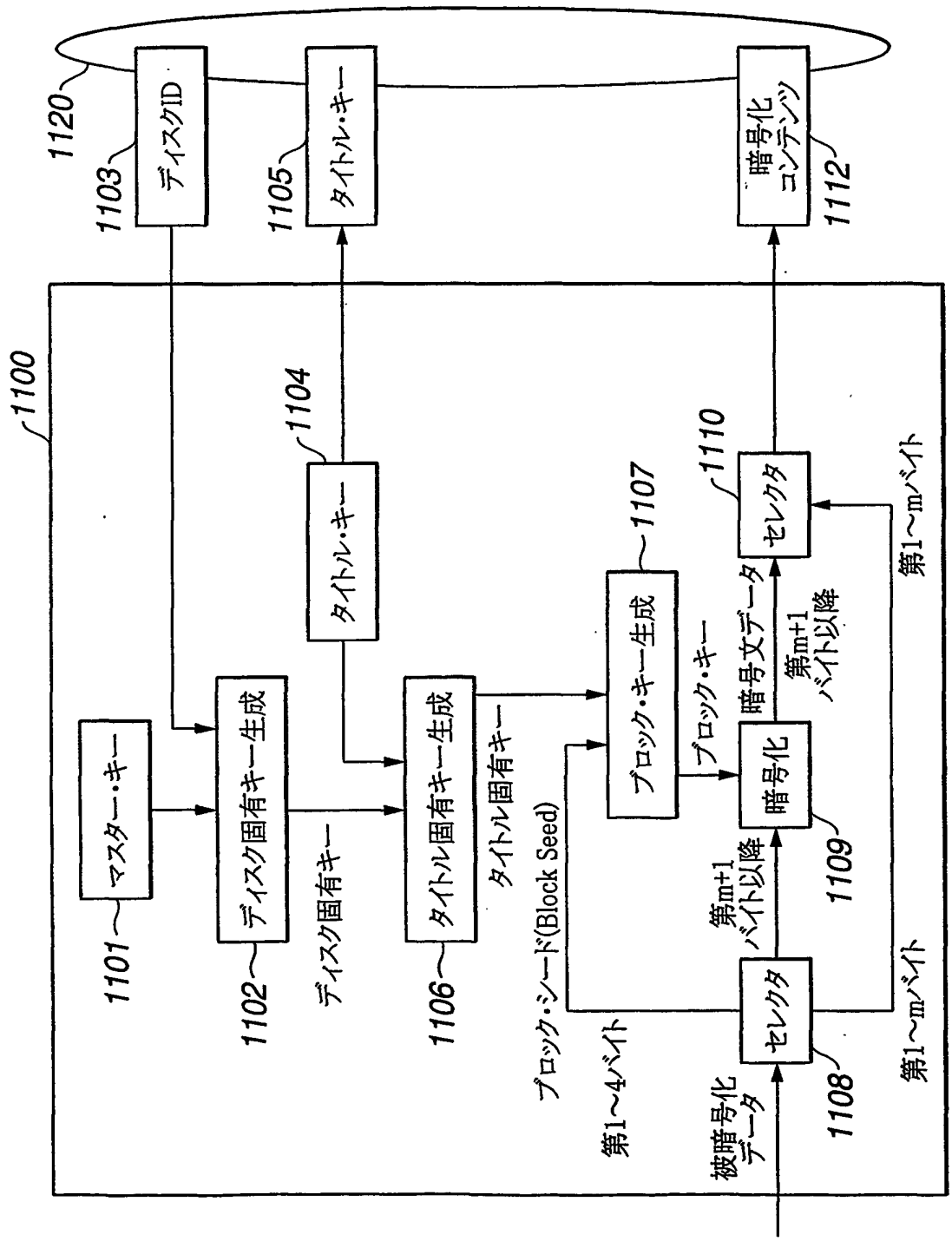

1120
1103
ディスクID
1105
タイトル・キー
暗号化
コンテンツ
1112
1100
1104
1101
マスター・キー
1102
ディスク固有キー生成
ディスク固有キー
1106
タイトル固有キー生成
タイトル固有キー
1107
ブロック・キー生成
ブロック・キー
1110
セレクタ
暗号文データ
第m+1
バイト以降
暗号化
1109
第m+1
バイト以降
ブロック・シード(Block Seed)
第1～4バイト
セレクタ
1108
被暗号化
データ
第1～mバイト
第1～mバイト

FIG.11

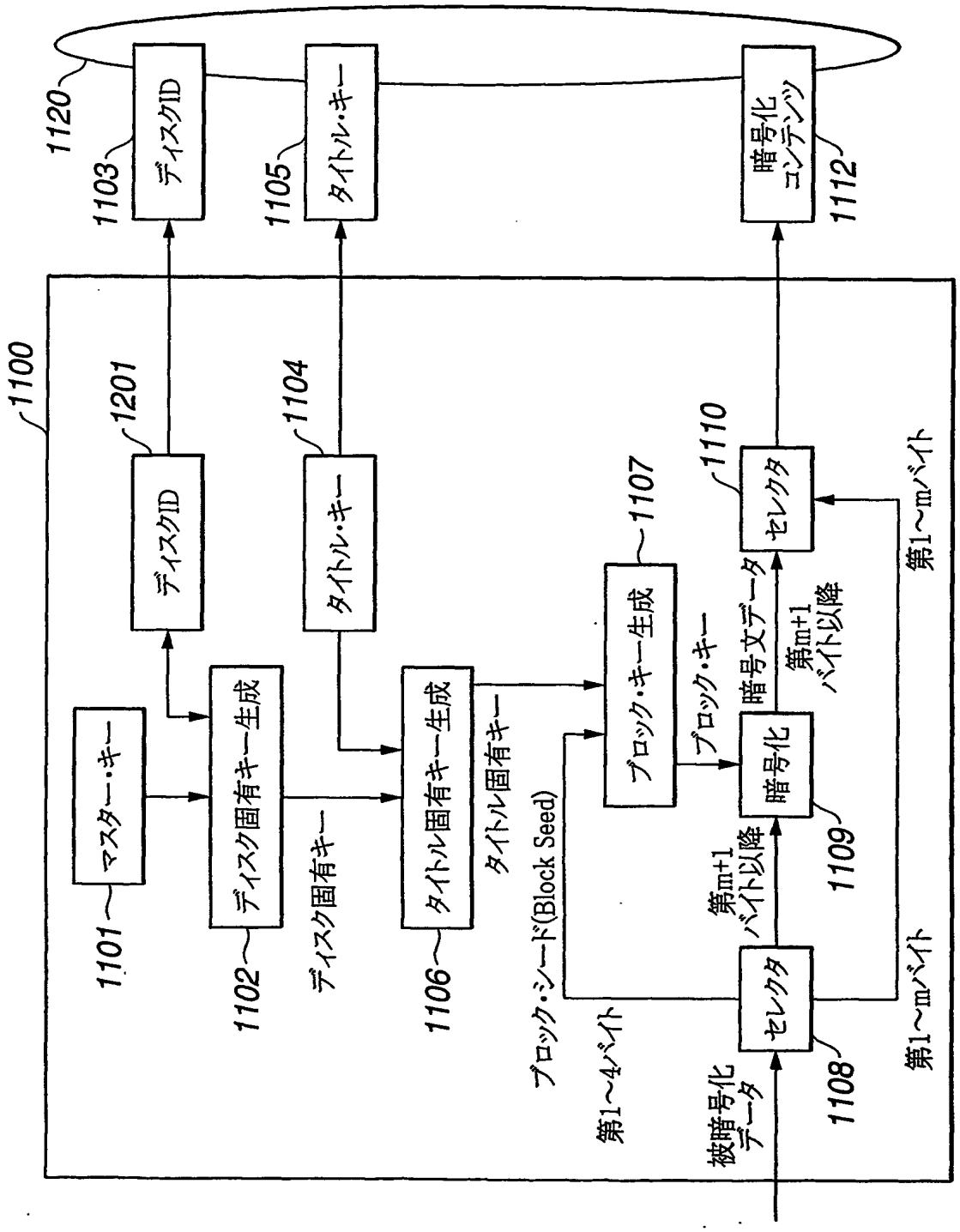

1120
1103
ディスクID
1105
タイトル・キー
暗号化コンテンツ
1112
1100
1201
ディスクID
1104
タイトル・キー
1107
1110
セレクタ
マスター・キー
1101
ディスク固有キー生成
1102
ディスク固有キー
タイトル固有キー生成
1106
タイトル固有キー
ブロック・シード(Block Seed)
ブロック・キー生成
ブロック・キー
暗号文データ
第m+1バイト以降
第1～mバイト
第1～4バイト
第m+1バイト以降
暗号化
1109
被暗号化データ
セレクタ
1108
第1～mバイト

FIG.12

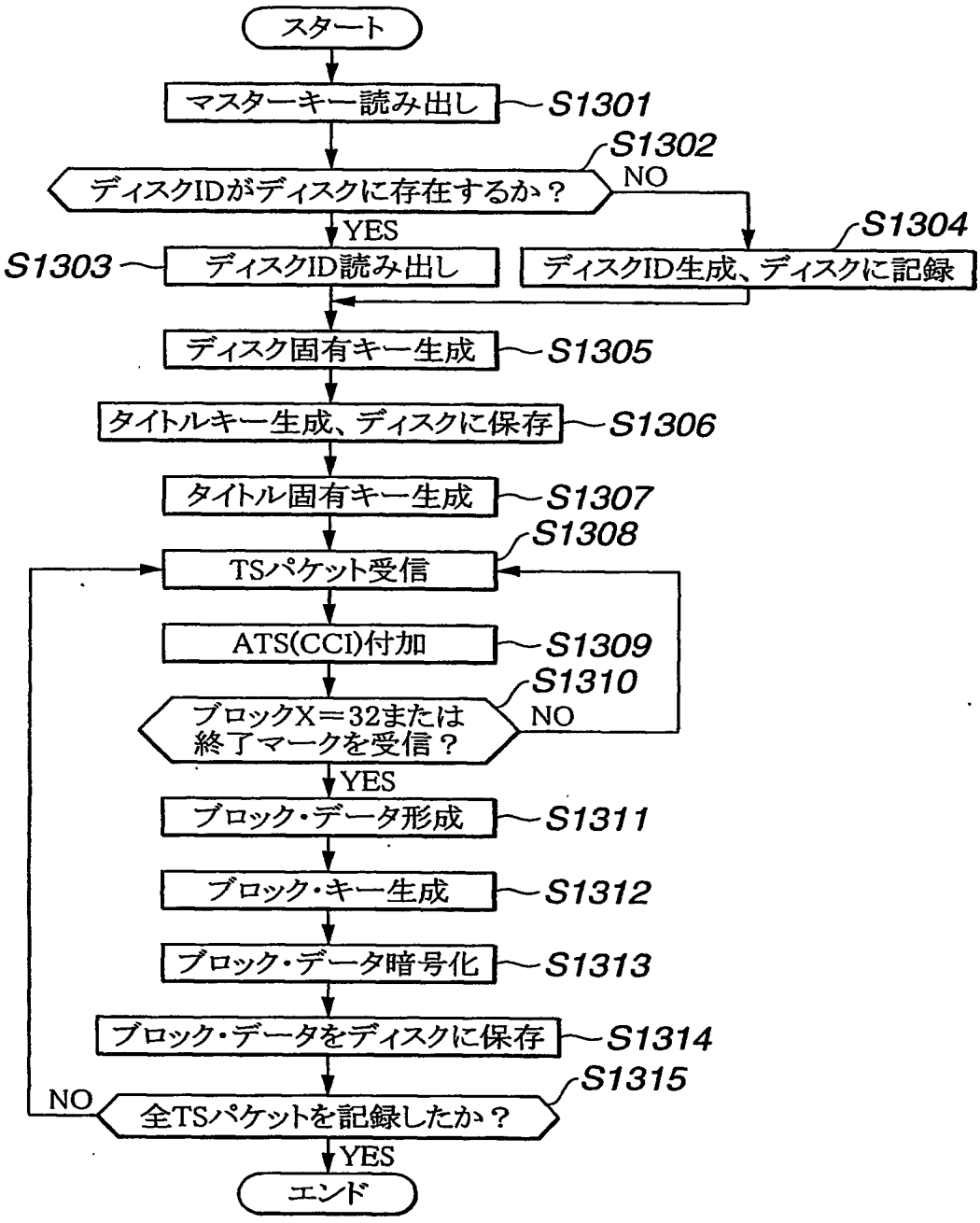

スタート
マスターキー読み出し
S1301
S1302
ディスクIDがディスクに存在するか？
NO
YES
S1303
ディスクID読み出し
S1304
ディスクID生成、ディスクに記録
ディスク固有キー生成
S1305
タイトルキー生成、ディスクに保存
S1306
タイトル固有キー生成
S1307
S1308
TSパケット受信
ATS(CCI)付加
S1309
S1310
ブロックX＝32または
終了マークを受信？
NO
YES
ブロック・データ形成
S1311
ブロック・キー生成
S1312
ブロック・データ暗号化
S1313
ブロック・データをディスクに保存
S1314
S1315
NO
全TSパケットを記録したか？
YES
エンド

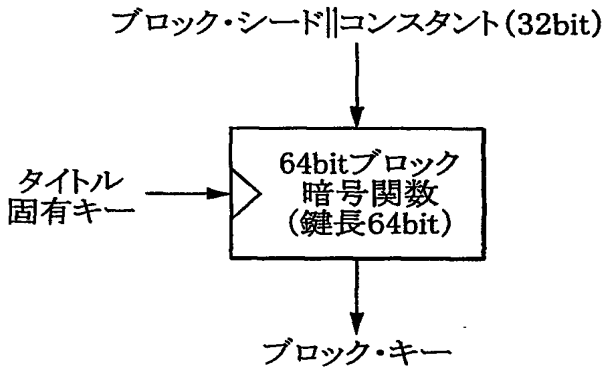
FIG.13

ブロック・キー生成例

入力
ブロック・シード(32bit)
タイトル固有キー(64bit)

出力
ブロック・キー(64bit)

例1



例2

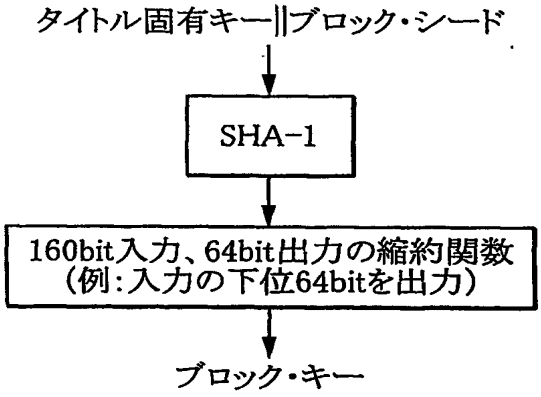


FIG.14

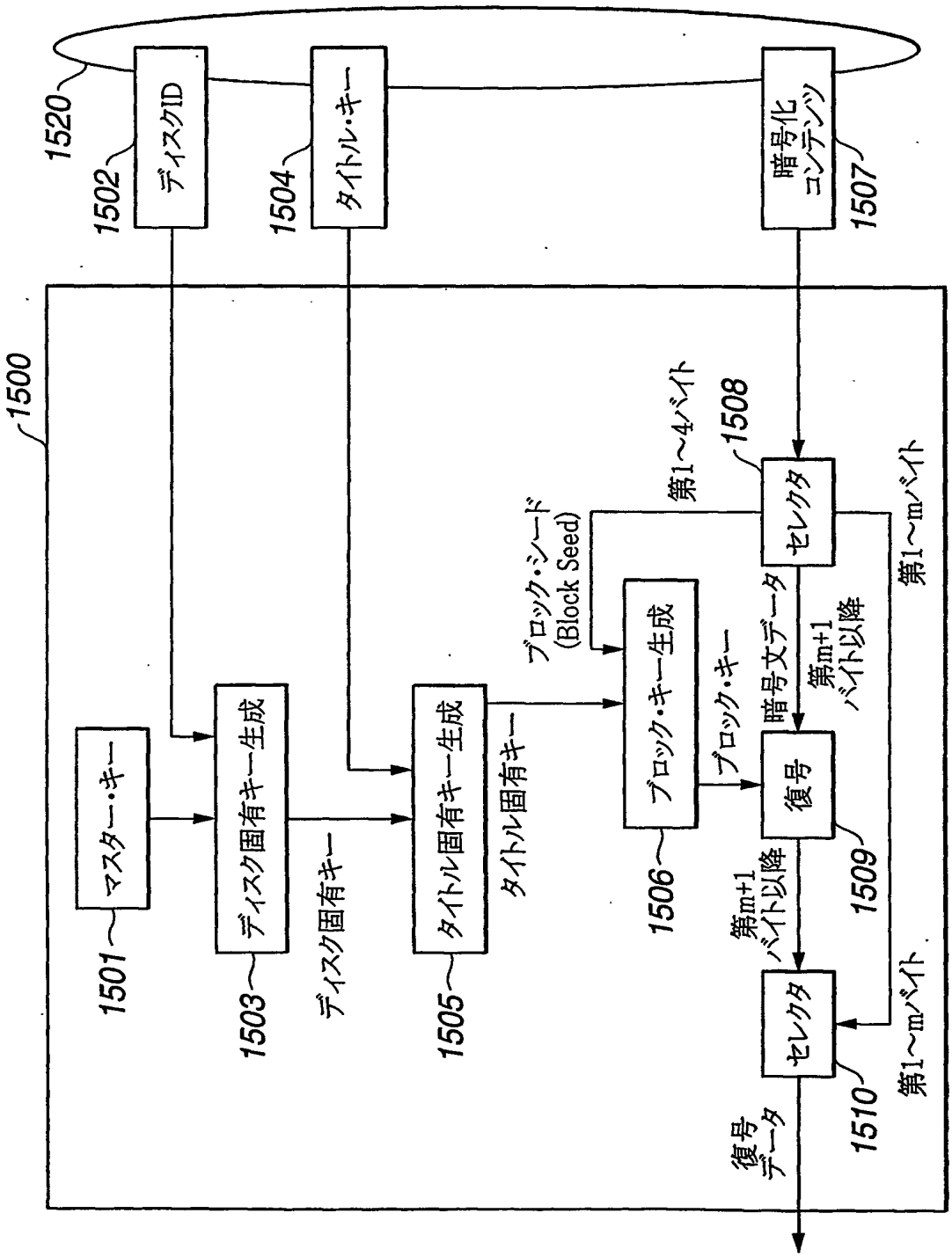

1520
1502
ディスクID
1504
タイトル・キー
1507
暗号化コンテンツ
1500
1501
マスター・キー
1503
ディスク固有キー生成
ディスク固有キー
1505
タイトル固有キー生成
タイトル固有キー
ブロック・シード (Block Seed)
1506
ブロック・キー生成
ブロック・キー
第1～4バイト
1508
セレクタ
暗号文データ
第m+1バイト以降
1509
復号
第m+1バイト以降
第1～mバイト
セレクタ
1510
第1～mバイト
復号データ

FIG.15

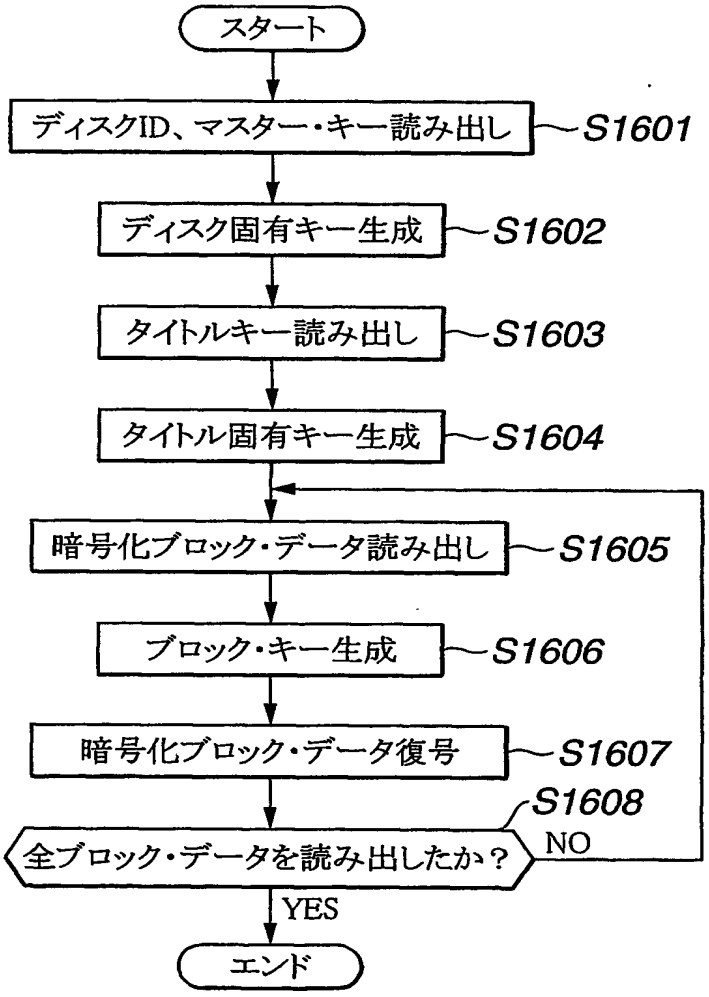

スタート
ディスクID、マスター・キー読み出し
S1601
ディスク固有キー生成
S1602
タイトルキー読み出し
S1603
タイトル固有キー生成
S1604
暗号化ブロック・データ読み出し
S1605
ブロック・キー生成
S1606
暗号化ブロック・データ復号
S1607
S1608
全ブロック・データを読み出したか？
NO
YES
エンド

FIG.16

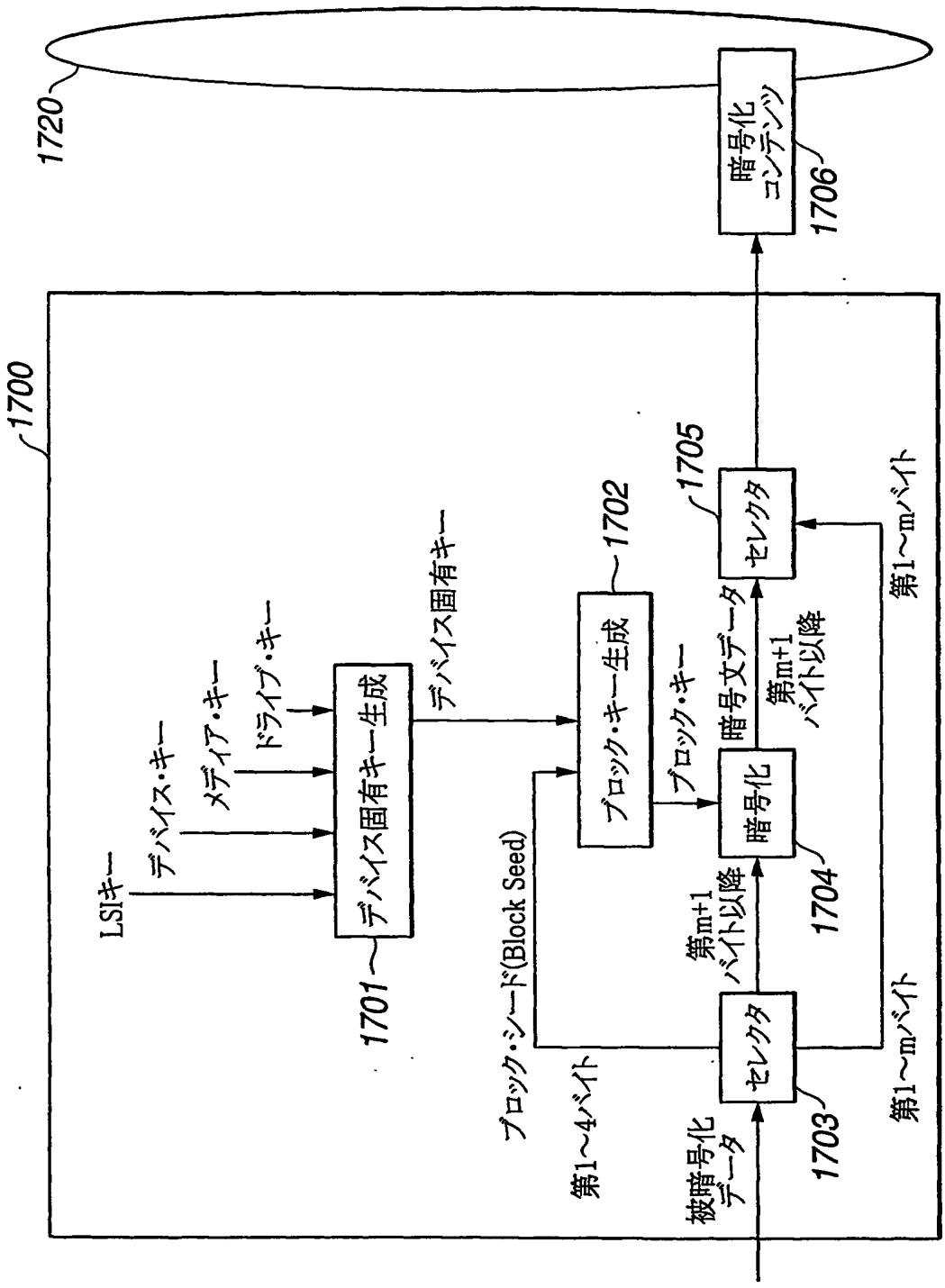

1720
暗号化コンテンツ
1706
1700
1705
セレクタ
1702
ブロック・キー生成
デバイス固有キー
1701
デバイス固有キー生成
LSIキー
デバイス・キー
メディア・キー
ドライブ・キー
ブロック・キー
暗号文データ
第m+1バイト以降
暗号化
1704
ブロック・シード(Block Seed)
第1～4バイト
第m+1バイト以降
セレクタ
1703
被暗号化データ
第1～mバイト
第1～mバイト

FIG.17

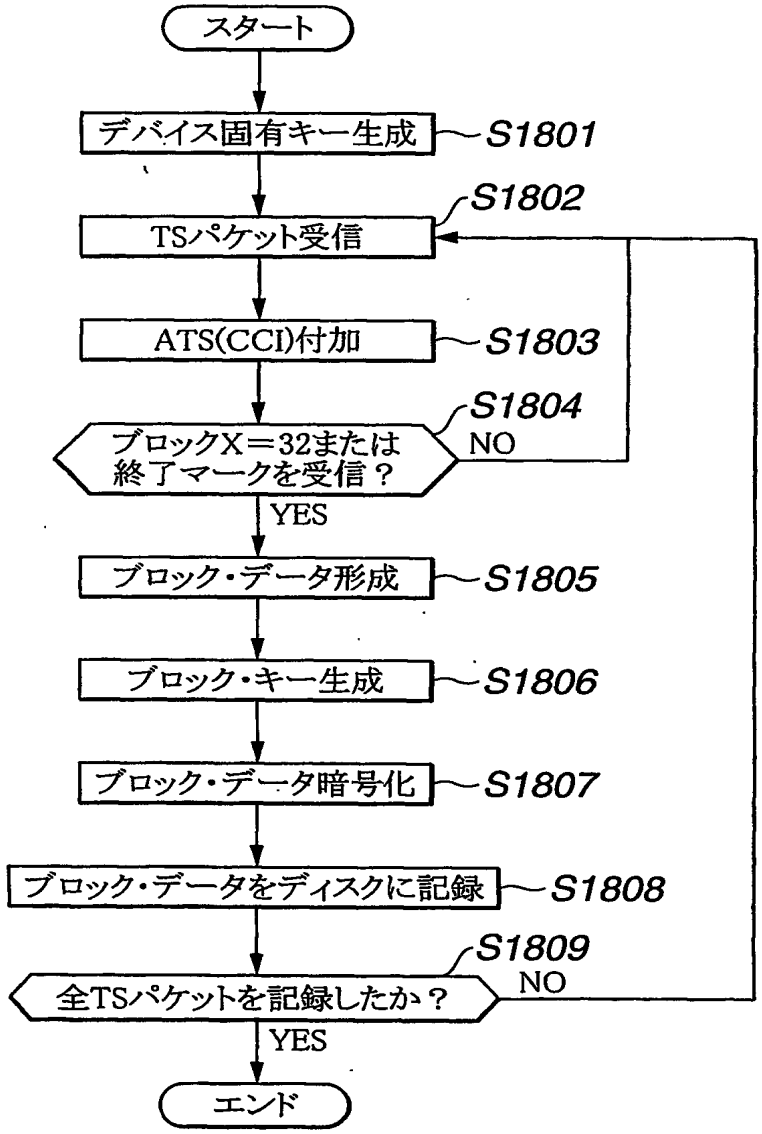

スタート
デバイス固有キー生成
S1801
S1802
TSパケット受信
ATS(CCI)付加
S1803
S1804
ブロックX＝32または
終了マークを受信？
NO
YES
ブロック・データ形成
S1805
ブロック・キー生成
S1806
ブロック・データ暗号化
S1807
ブロック・データをディスクに記録
S1808
S1809
全TSパケットを記録したか？
NO
YES
エンド

FIG.18

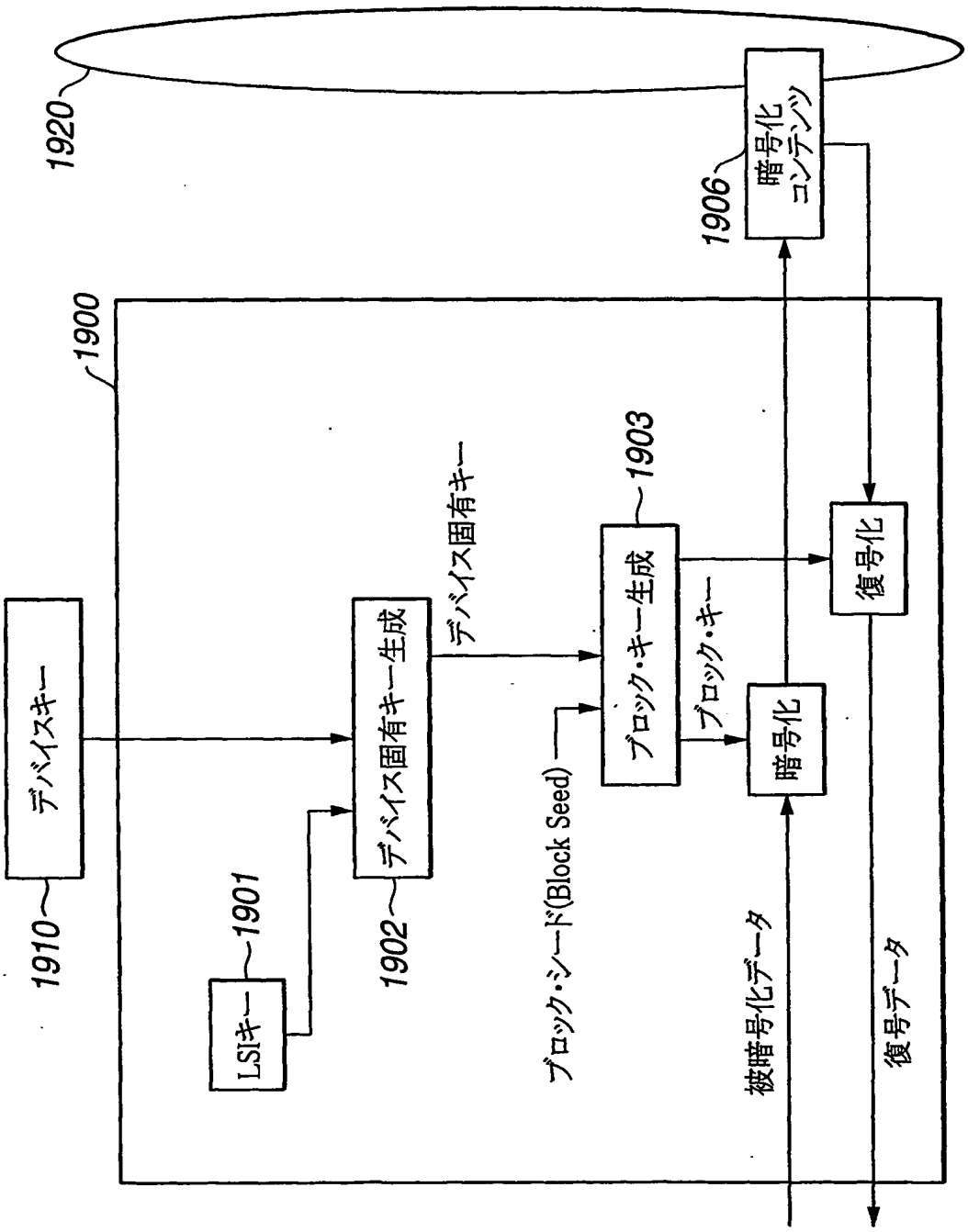

1920
1906
暗号化
コンテンツ
1900
デバイスキー
1910
LSIキー
1901
デバイス固有キー生成
1902
デバイス固有キー
ブロック・シード(Block Seed)
ブロック・キー生成
1903
ブロック・キー
暗号化
復号化
被暗号化データ
復号データ

FIG.19

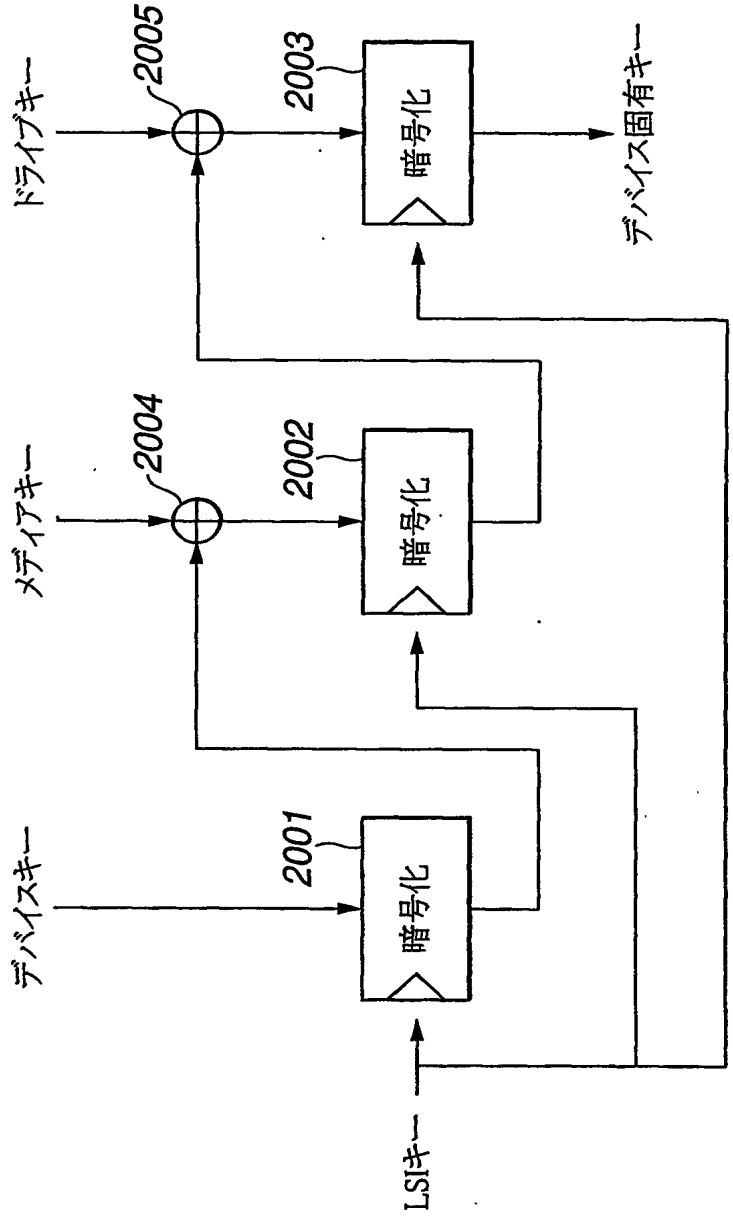

ドライブキー
2005
2003
暗号化
デバイス固有キー
メディアキー
2004
2002
暗号化
デバイスキー
2001
暗号化
LSIキー

FIG.20

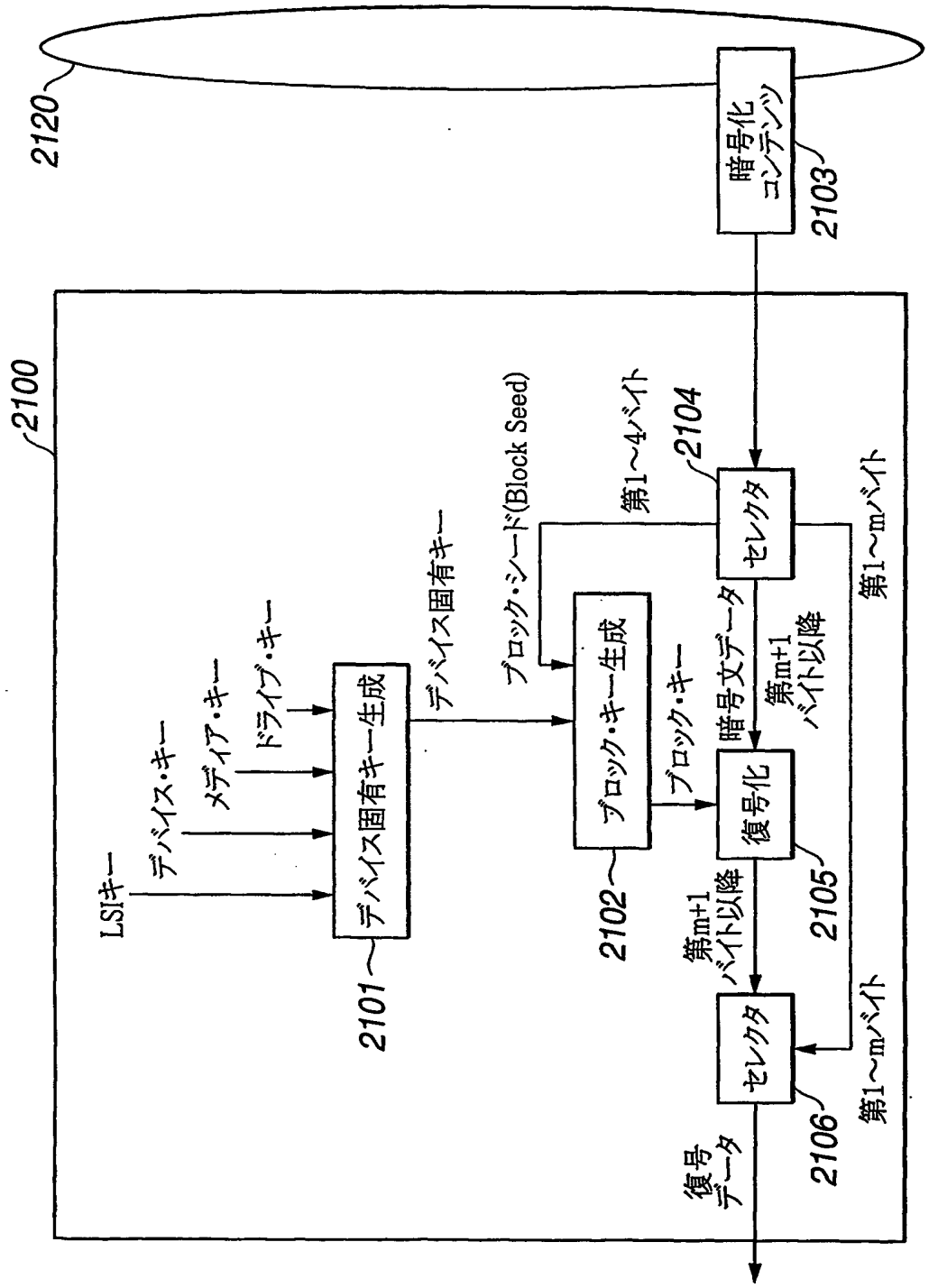

2120
暗号化コンテンツ
2103
2100
LSIキー
デバイス・キー
メディア・キー
ドライブ・キー
デバイス固有キー生成
2101
デバイス固有キー
ブロック・シード(Block Seed)
第1～4バイト
2104
セレクタ
ブロック・キー生成
2102
ブロック・キー
暗号文データ
第m+1バイト以降
第1～mバイト
復号化
2105
第m+1バイト以降
セレクタ
2106
第1～mバイト
復号データ

FIG.21

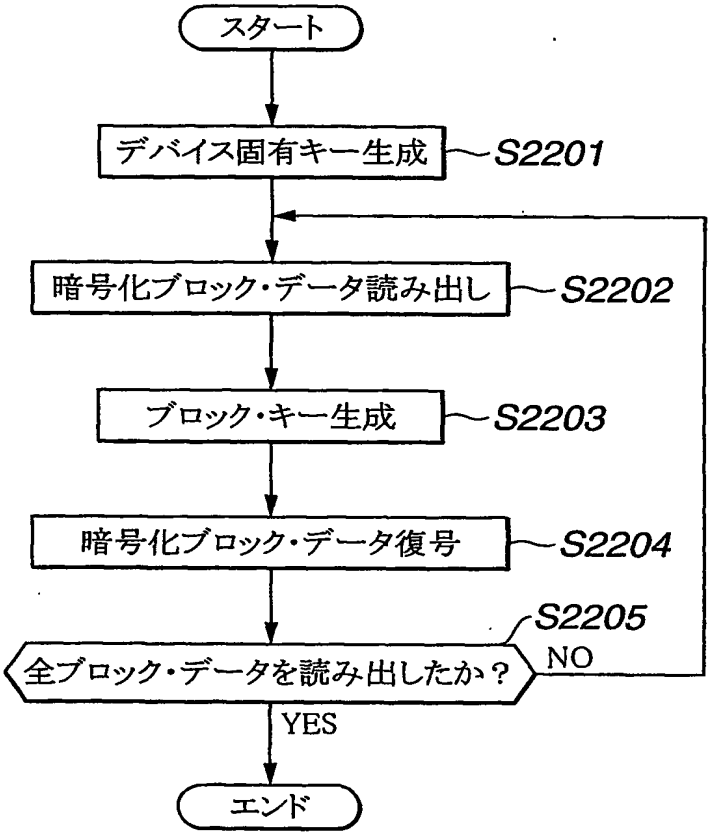

スタート
デバイス固有キー生成
S2201
暗号化ブロック・データ読み出し
S2202
ブロック・キー生成
S2203
暗号化ブロック・データ復号
S2204
S2205
全ブロック・データを読み出したか？
NO
YES
エンド

FIG.22

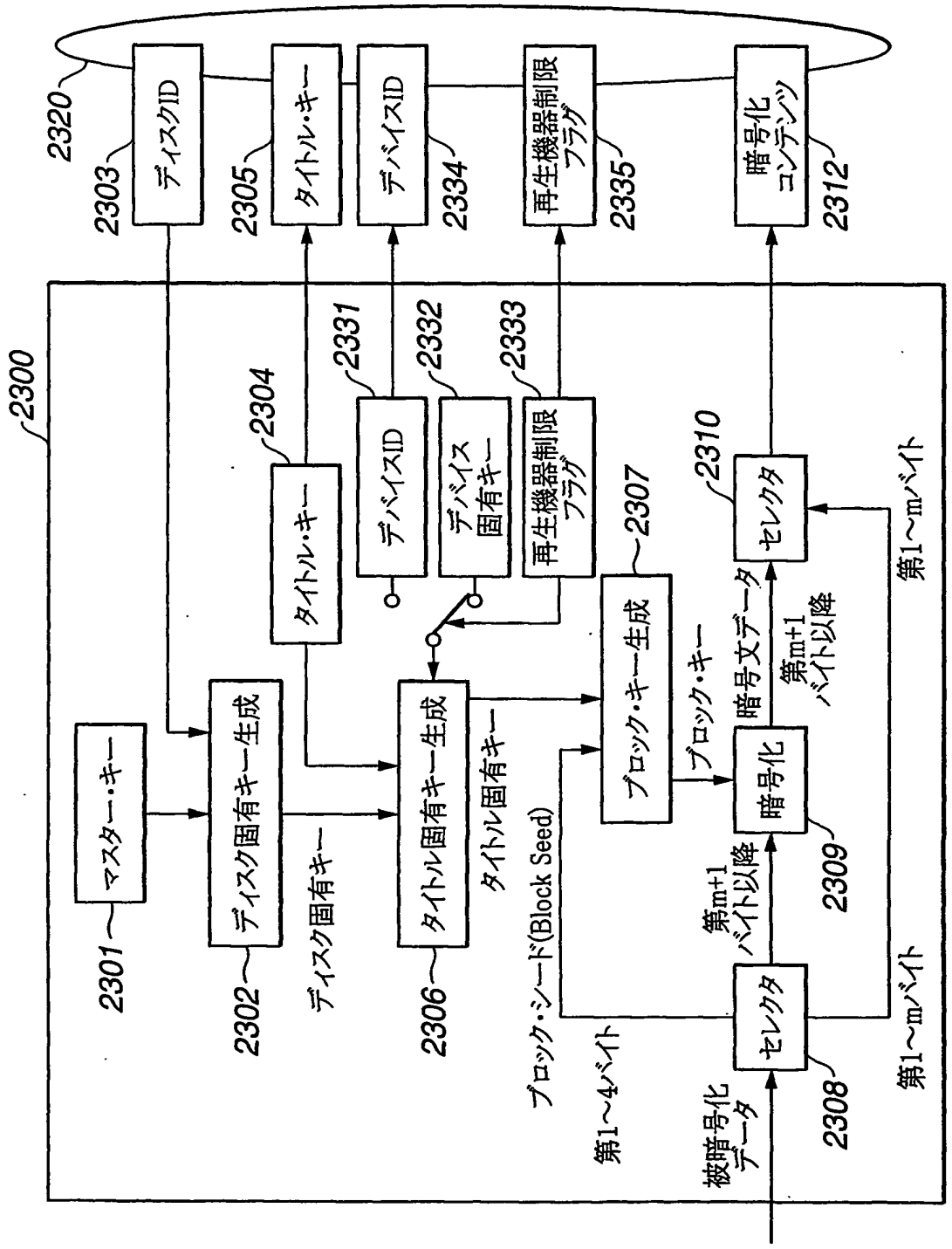

2320
2303
ディスクID
2305
タイトル・キー
2334
デバイスID
2335
再生機器制限フラグ
2312
暗号化コンテンツ
2300
2304
タイトル・キー
2331
デバイスID
2332
デバイス固有キー
2333
再生機器制限フラグ
2307
ブロック・キー生成
2310
セレクタ
2301
マスター・キー
2302
ディスク固有キー生成
ディスク固有キー
2306
タイトル固有キー生成
タイトル固有キー
ブロック・シード(Block Seed)
第1～4バイト
ブロック・キー
暗号文データ
第m+1バイト以降
第m+1バイト以降
2309
暗号化
第1～mバイト
第1～mバイト
被暗号化データ
2308
セレクタ

FIG.23

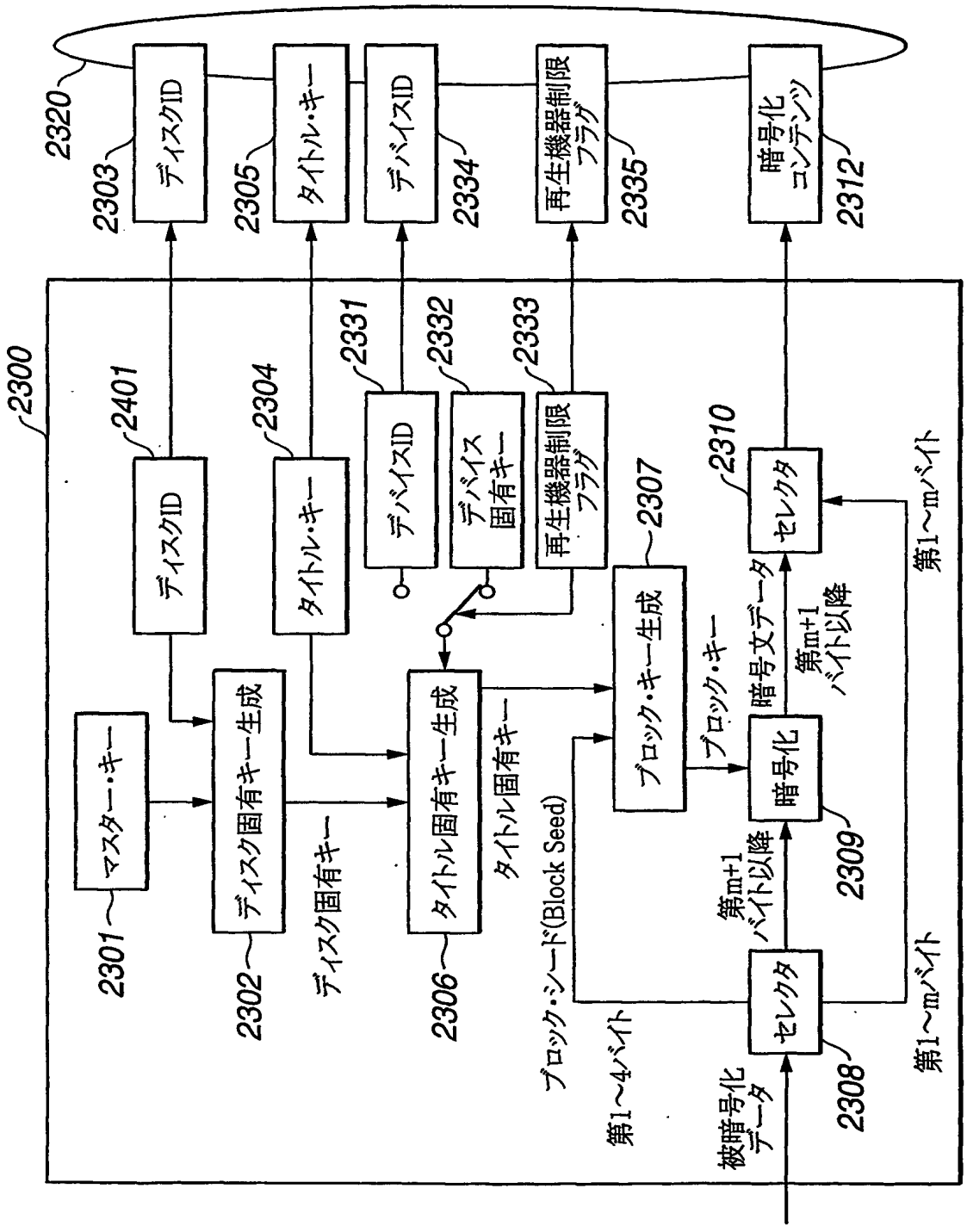

2320
2303
ディスクID
2305
タイトル・キー
2334
デバイスID
2335
再生機器制限フラグ
2312
暗号化コンテンツ
2300
2401
ディスクID
2304
タイトル・キー
2331
デバイスID
2332
デバイス固有キー
2333
再生機器制限フラグ
2307
2310
セレクタ
2301
マスター・キー
2302
ディスク固有キー生成
ディスク固有キー
2306
タイトル固有キー生成
タイトル固有キー
ブロック・シード(Block Seed)
ブロック・キー生成
ブロック・キー
暗号文データ
第m+1バイト以降
第1～mバイト
第1～4バイト
第m+1バイト以降
暗号化
2309
セレクタ
被暗号化データ
2308
第1～mバイト

FIG.24

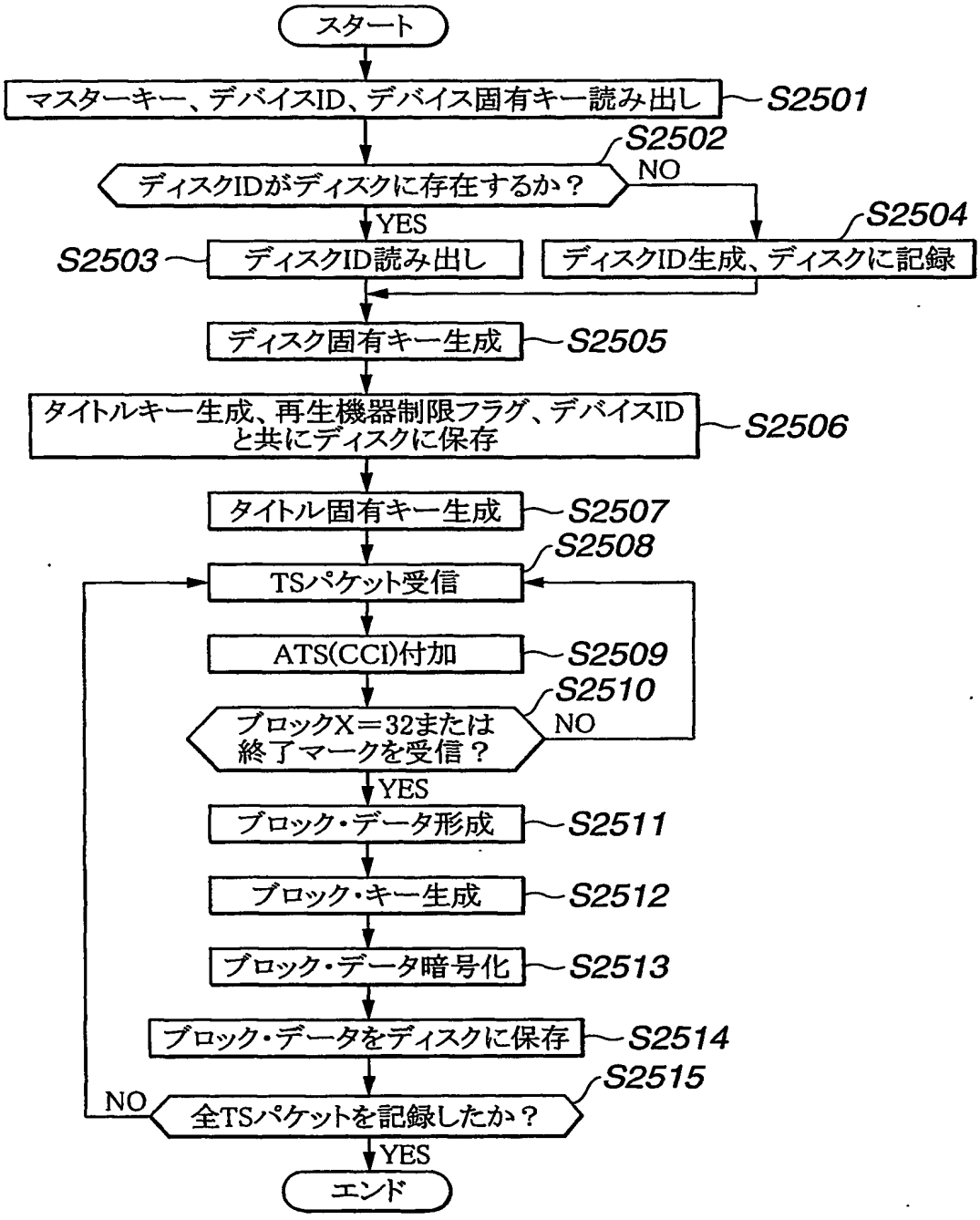

スタート
マスターキー、デバイスID、デバイス固有キー読み出し
S2501
S2502
ディスクIDがディスクに存在するか？
NO
YES
S2504
S2503
ディスクID読み出し
ディスクID生成、ディスクに記録
ディスク固有キー生成
S2505
タイトルキー生成、再生機器制限フラグ、デバイスID
と共にディスクに保存
S2506
タイトル固有キー生成
S2507
S2508
TSパケット受信
ATS(CCI)付加
S2509
S2510
ブロックX＝32または
終了マークを受信？
NO
YES
ブロック・データ形成
S2511
ブロック・キー生成
S2512
ブロック・データ暗号化
S2513
ブロック・データをディスクに保存
S2514
S2515
NO
全TSパケットを記録したか？
YES
エンド

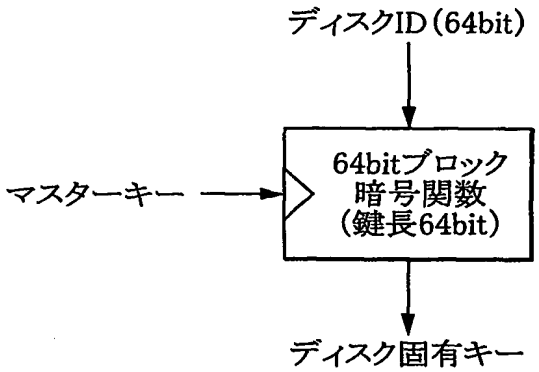
FIG.25

ディスク固有キー生成例

入力
マスターキー(64bit)
ディスクID(64bit)

出力
ディスク固有キー(64bit)

例1



例2

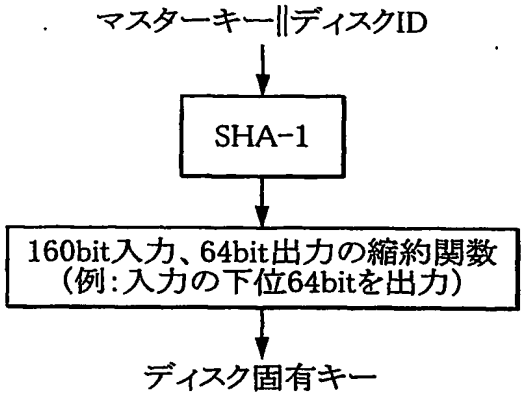


FIG.26

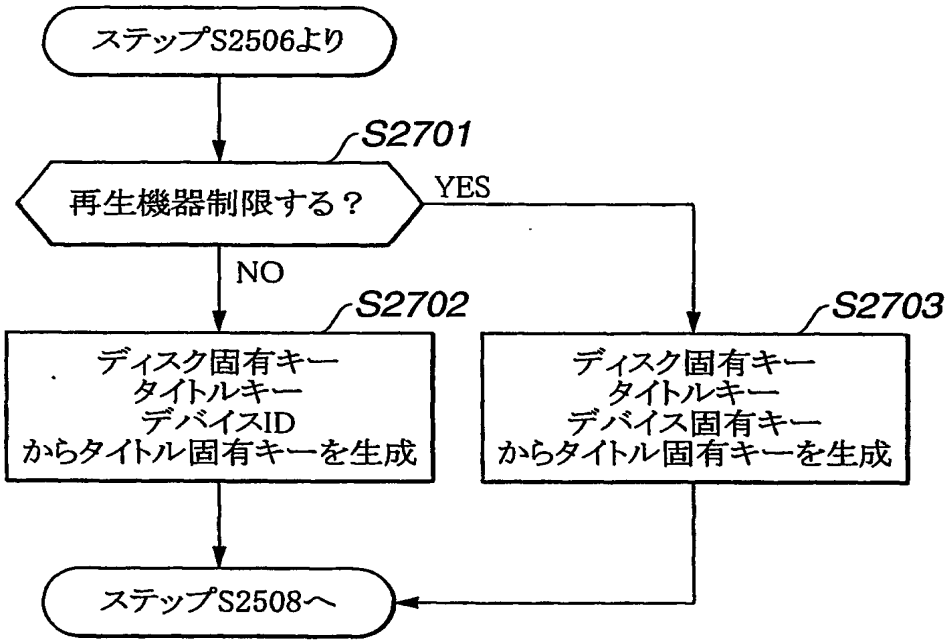

ステップS2506より
S2701
再生機器制限する？
YES
NO
S2702
ディスク固有キー
タイトルキー
デバイスID
からタイトル固有キーを生成
S2703
ディスク固有キー
タイトルキー
デバイス固有キー
からタイトル固有キーを生成
ステップS2508へ

FIG.27

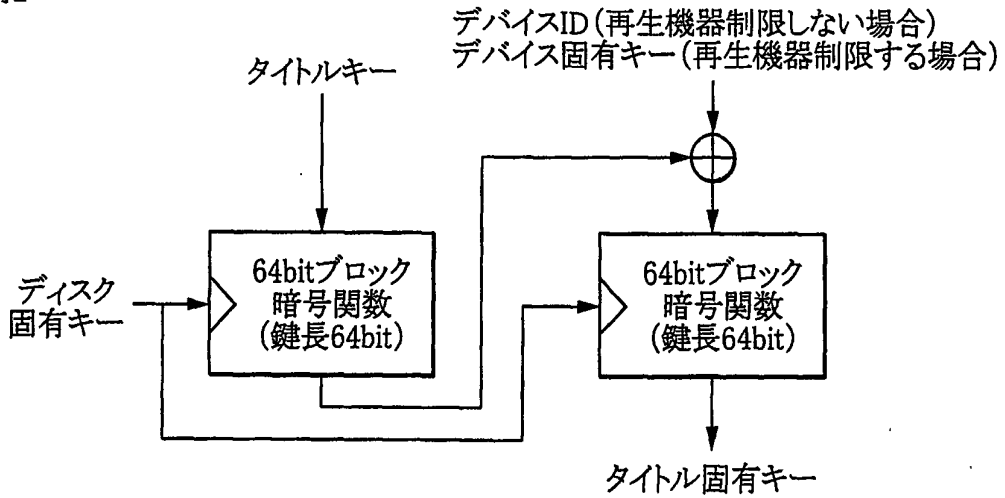
タイトル固有キー生成例

入力
ディスク固有キー(64bit)
タイトルキー(64bit)

ディスクID(64bit)または
デバイス固有キー(64bit)

出力
タイトル固有キー(64bit)

例1



例2

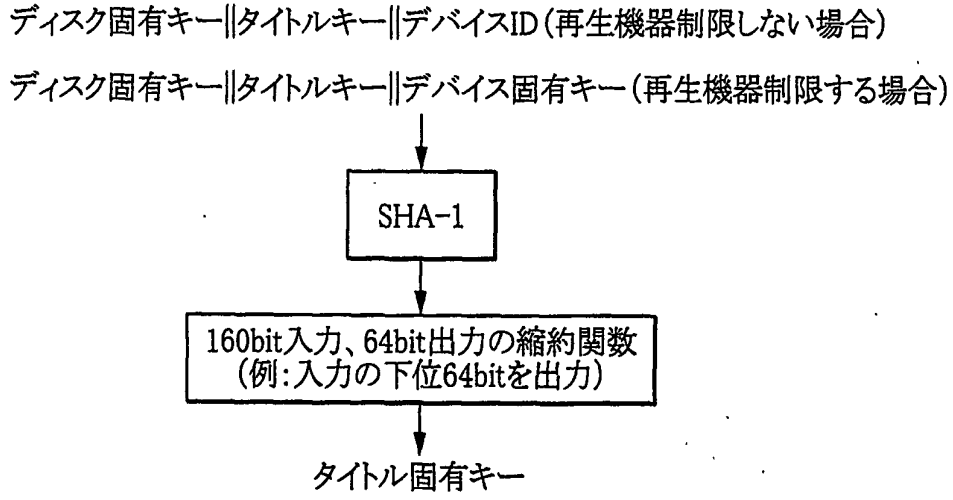


FIG.28

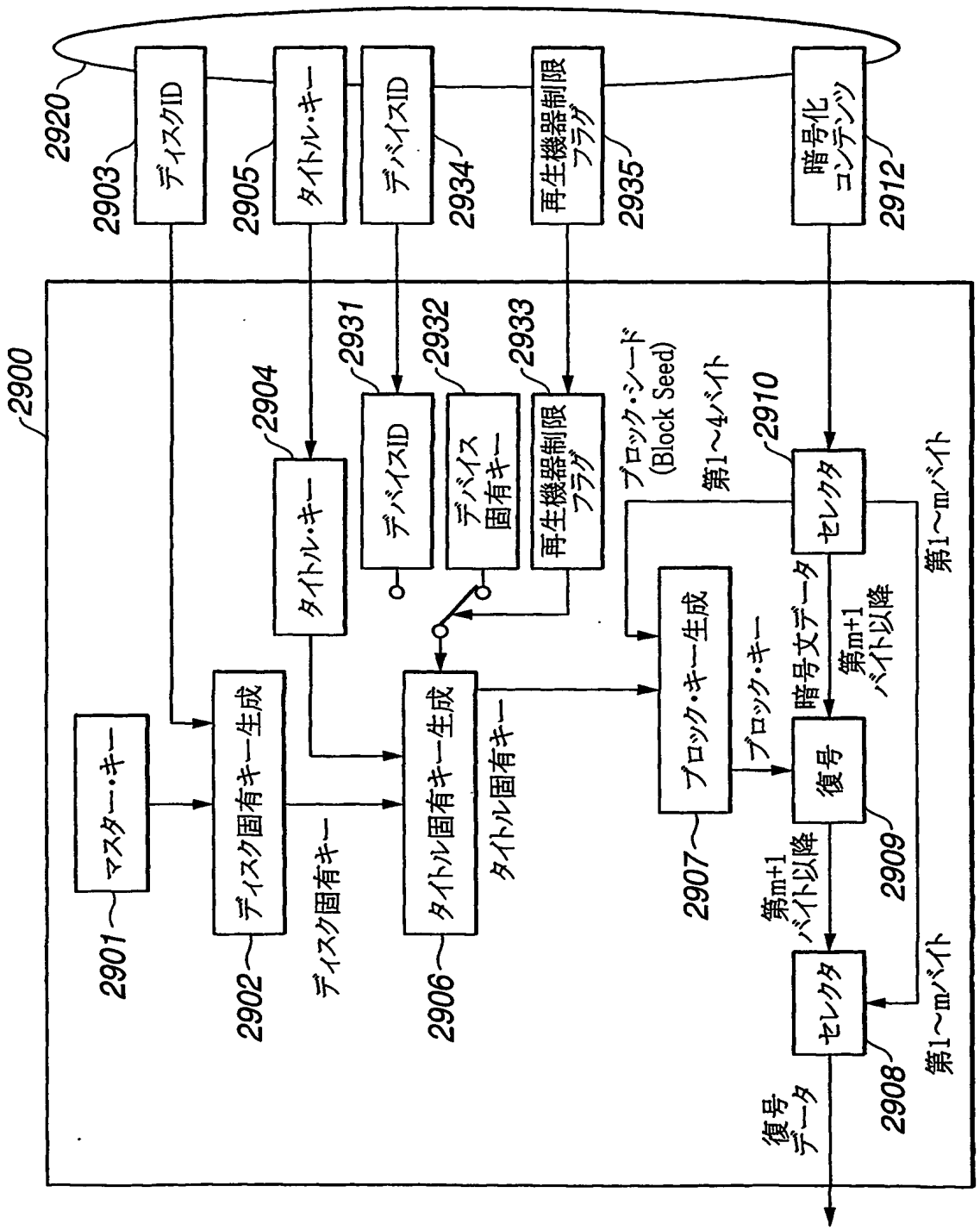

2920
2903
ディスクID
2905
タイトル・キー
2934
デバイスID
2935
再生機器制限フラグ
2912
暗号化コンテンツ
2900
2931
2932
2933
2904
タイトル・キー
デバイスID
デバイス固有キー
再生機器制限フラグ
ブロック・シード (Block Seed)
第1～4バイト
2910
セレクタ
第1～mバイト
マスター・キー
2901
ディスク固有キー生成
2902
ディスク固有キー
タイトル固有キー生成
2906
タイトル固有キー
ブロック・キー生成
2907
ブロック・キー
暗号文データ
第m+1バイト以降
復号
2909
第m+1バイト以降
セレクタ
2908
第1～mバイト
復号データ

FIG.29

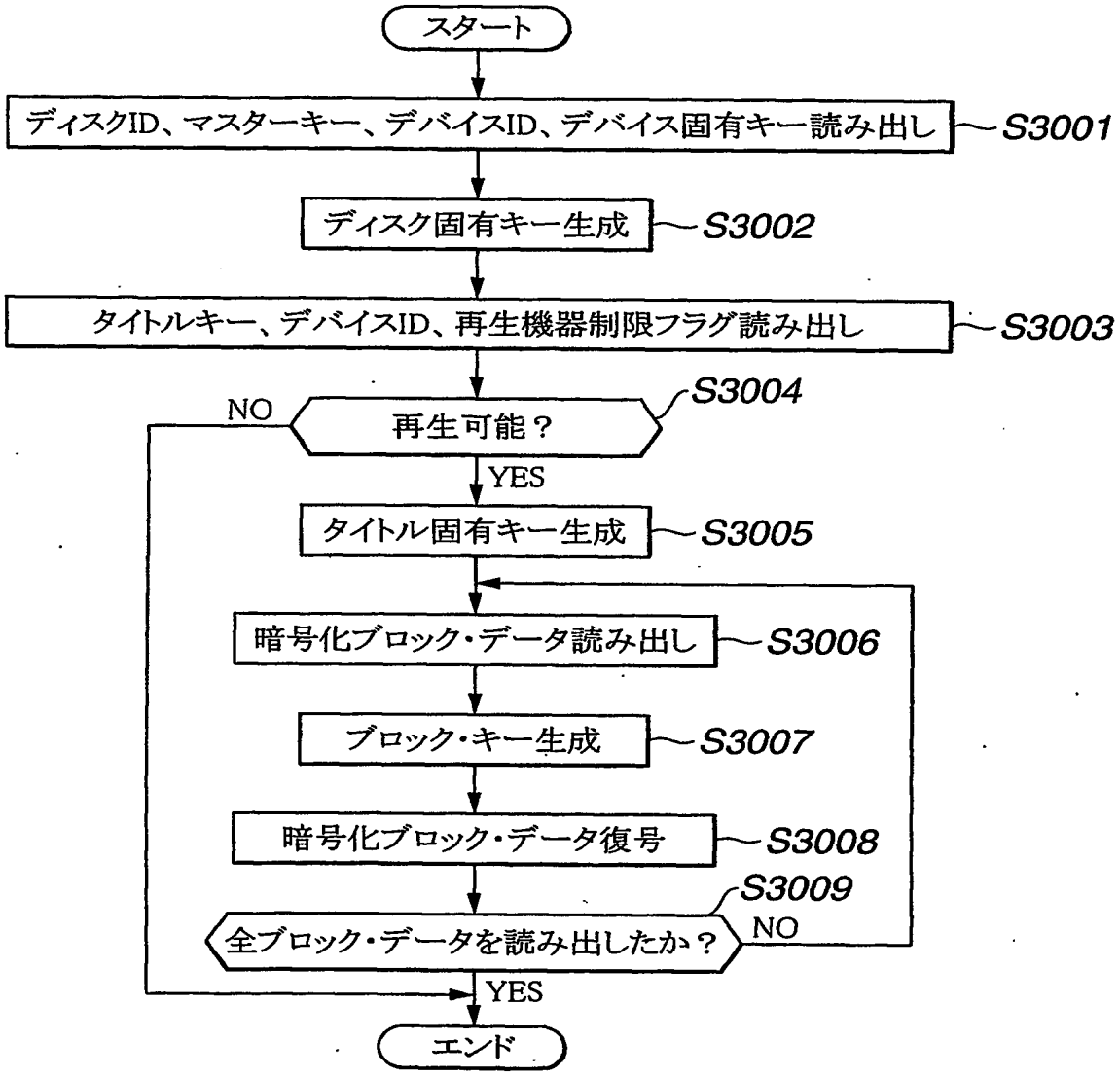

スタート
ディスクID、マスターキー、デバイスID、デバイス固有キー読み出し
S3001
ディスク固有キー生成
S3002
タイトルキー、デバイスID、再生機器制限フラグ読み出し
S3003
再生可能？
S3004
NO
YES
タイトル固有キー生成
S3005
暗号化ブロック・データ読み出し
S3006
ブロック・キー生成
S3007
暗号化ブロック・データ復号
S3008
全ブロック・データを読み出したか？
S3009
NO
YES
エンド

FIG.30

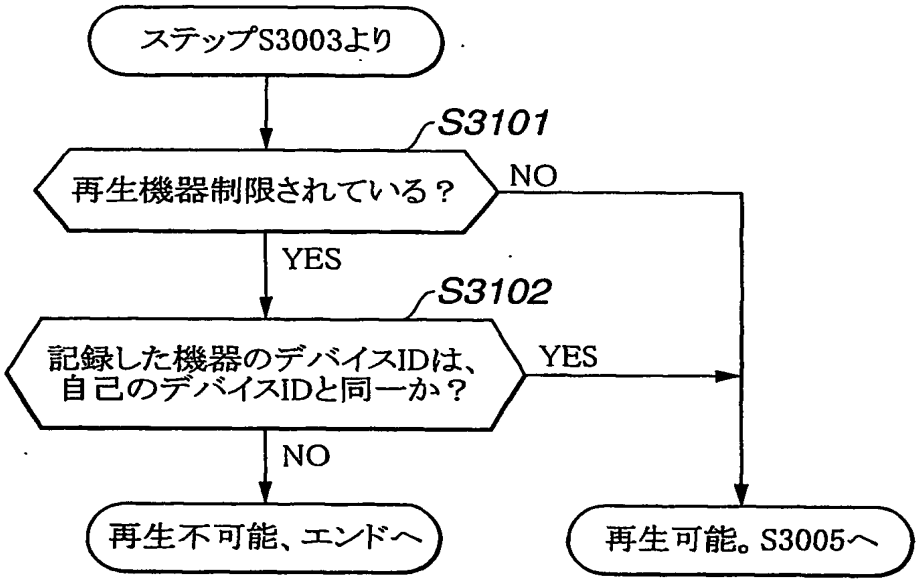

ステップS3003より
S3101
再生機器制限されている？
NO
YES
S3102
記録した機器のデバイスIDは、
自己のデバイスIDと同一か？
YES
NO
再生不可能、エンドへ
再生可能。S3005へ

FIG.31

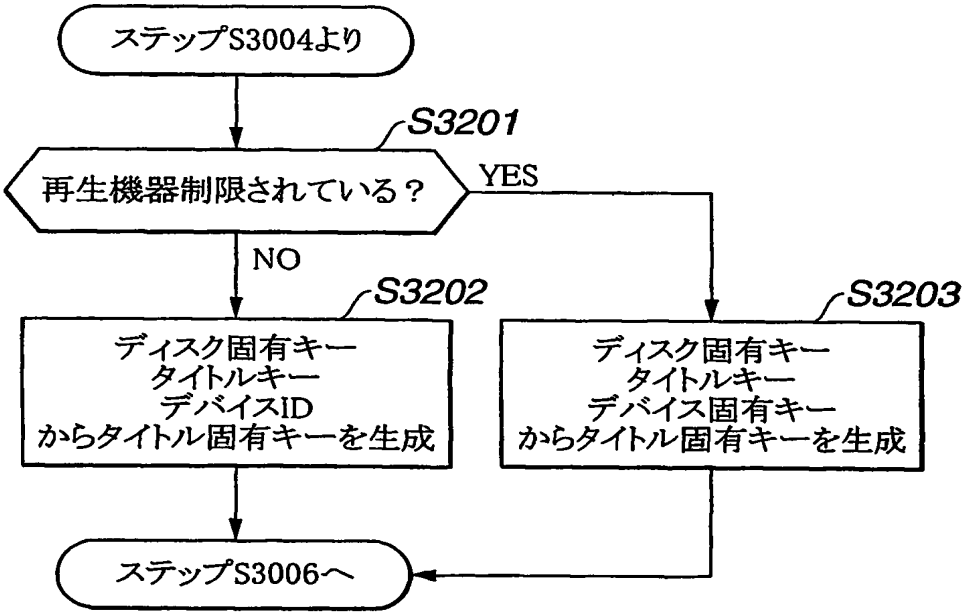

ステップS3004より
S3201
再生機器制限されている？
YES
NO
S3202
ディスク固有キー
タイトルキー
デバイスID
からタイトル固有キーを生成
S3203
ディスク固有キー
タイトルキー
デバイス固有キー
からタイトル固有キーを生成
ステップS3006へ

FIG.32

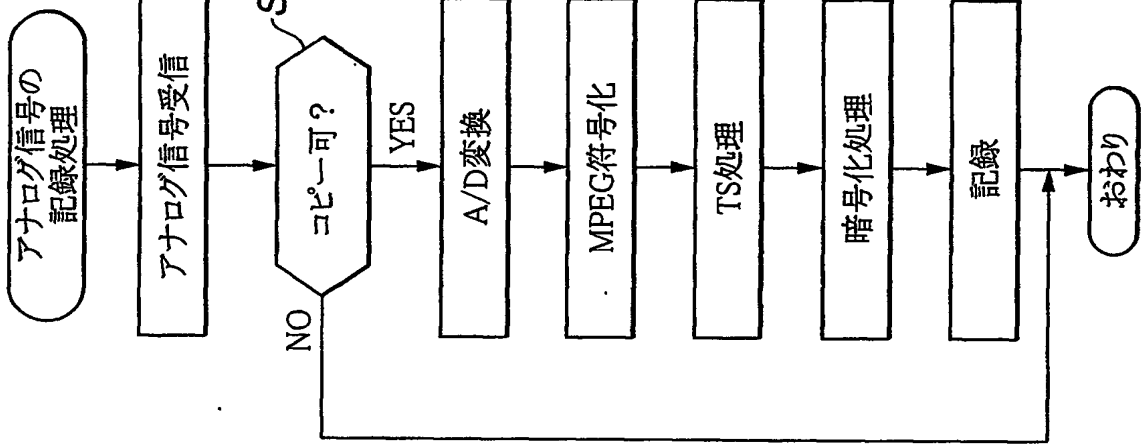


FIG.33B

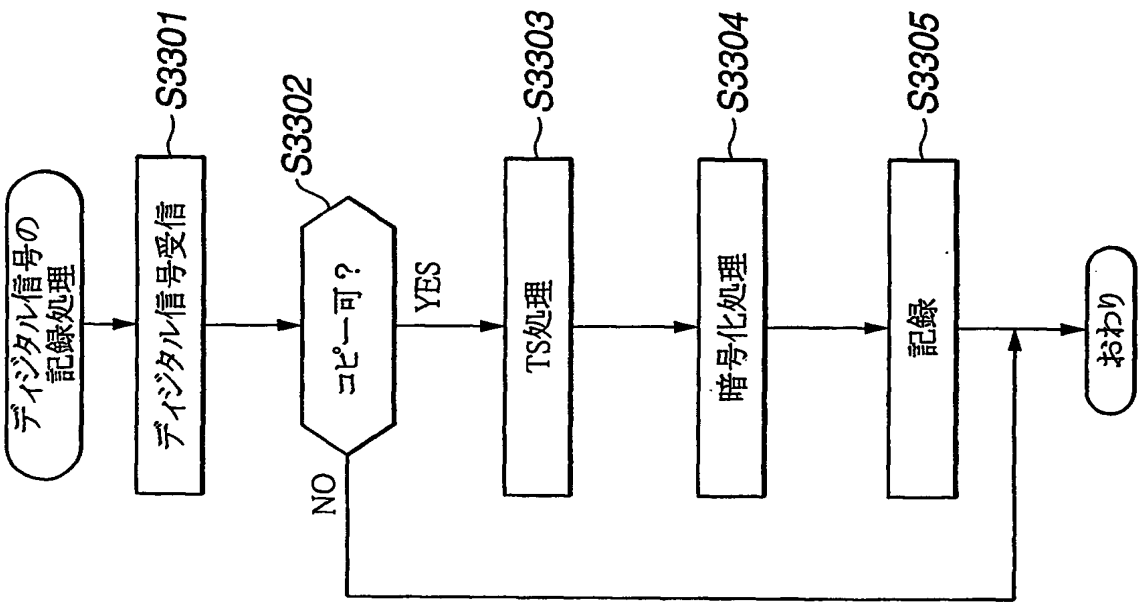


FIG.33A

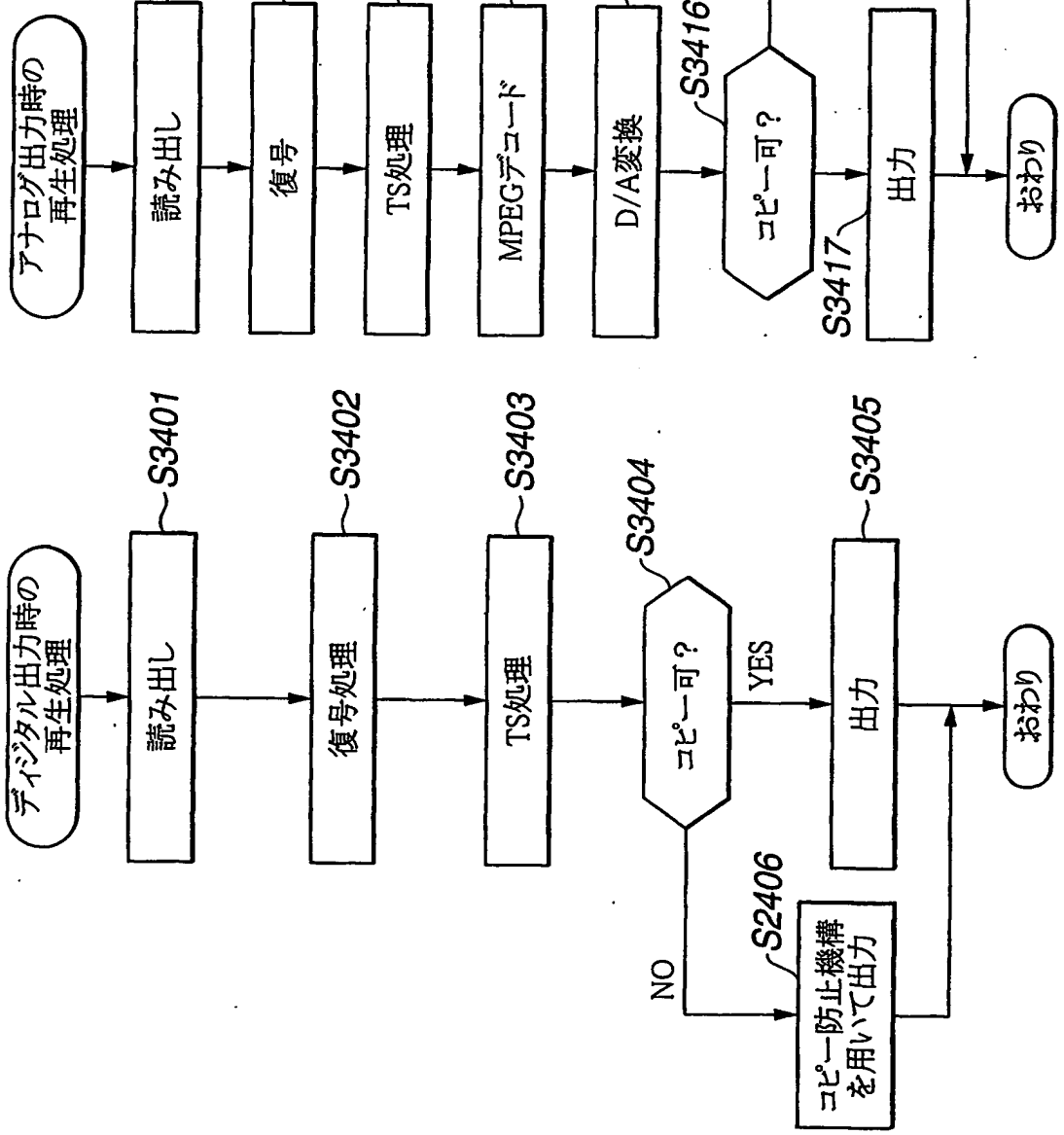


FIG.34A

FIG.34B

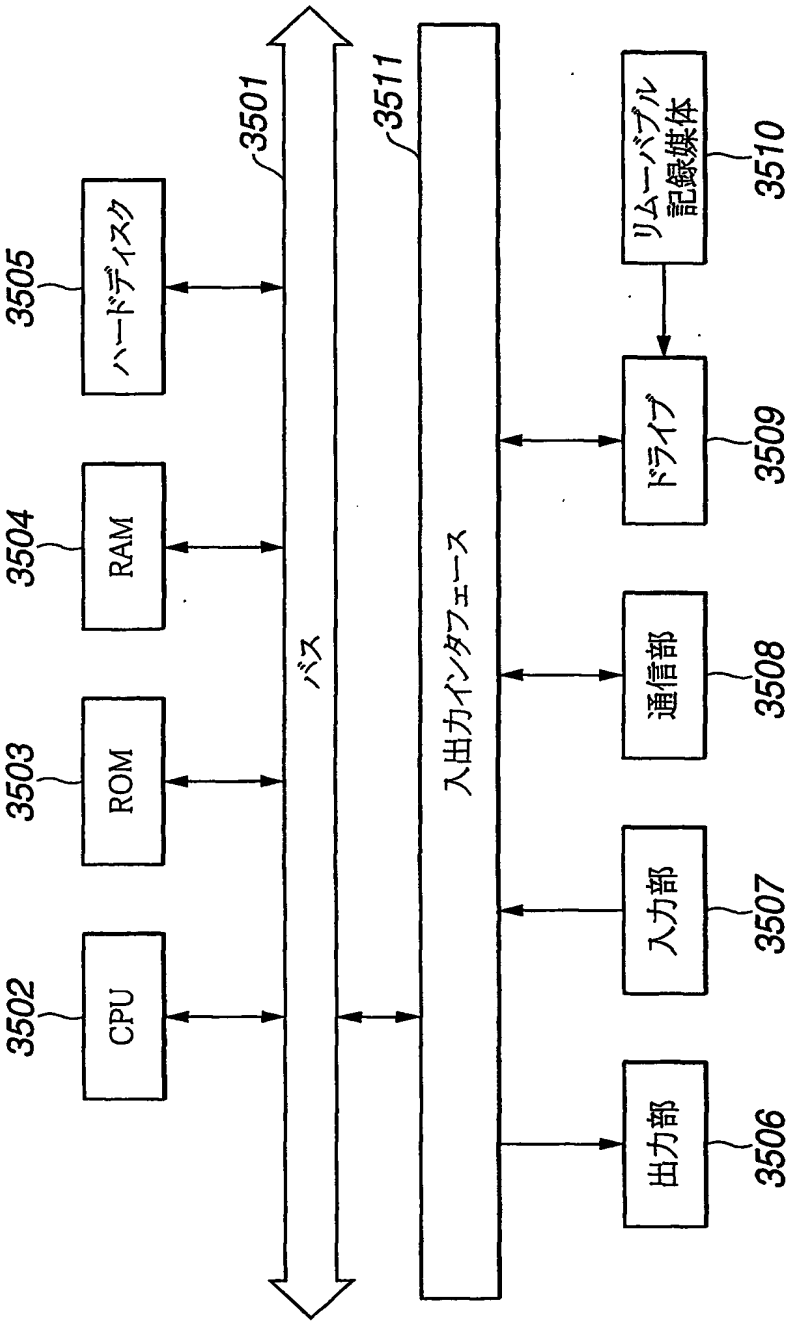

3501
3511
3505
ハードディスク
3504
RAM
3503
ROM
3502
CPU
バス
入出力インタフェース
リムーバブル記録媒体
3510
ドライブ
3509
通信部
3508
入力部
3507
出力部
3506

FIG.35

国際調査報告

国際出願番号　PCT／JP01／02928

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷　H04L9／00, G11B20／10, G11B20／12

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷　H04L9／00, G11B20／10, G11B20／12, G09C1／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2001年
日本国登録実用新案公報	1994－2001年
日本国実用新案登録公報	1996－2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

WPI, JICST科学技術文献データベース　cipher, encryption, DVD, timestamp

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP 11-224456 A (ソニー株式会社) 17.8月.1999(17.08.99), 第10欄第30－42行, 第11欄第40行-第12欄第2行, 図6 (ファミリーなし)	1-47
A	EP 874503 A2 (Sony CORP.) 28.10月.1998(28.10.98), 第6欄第49行－第7欄第57行 & JP 10-303945 A, 第11欄第34行－第12欄第46行 & KR 98081633 A	1-47
A	EP 924930 A2 (Hitachi, Ltd.) 30.11月.1998(30.11.98), 第9欄第57行－第10欄第44行, 図4,7 & JP 11-176091 A, 第12欄第36行－第13欄第26行, 図4,7	1-47

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日　04.07.01	国際調査報告の発送日　17.07.01
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 中里　裕正　5M　9364 電話番号　03－3581－1101　内線　3597

様式PCT／ISA／210（第2ページ）（1998年7月）